Oracle Integrated Lights Out Manager (ILOM) 3.1

Guía de configuración y mantenimiento

Referencia: E35730–01
Mayo de 2012



120808@25097

Contenido

Cómo utilizar esta documentación

Esta guía de configuración y mantenimiento proporciona información de la interfaz web y la CLI sobre las tareas de configuración y mantenimiento de Oracle ILOM.

Utilice esta guía junto con otras guías de la biblioteca de documentación de Oracle ILOM 3.1. Los destinatarios de esta guía son los técnicos, administradores de sistema, proveedores de servicio autorizados y usuarios que tengan experiencia en la administración de hardware de sistemas.

- "Documentación relacionada" en la página 7
- "Comentarios sobre este documento" en la página 8
- "Descargas de producto" en la página 8
- "Esquema de numeración de versiones de firmware de Oracle ILOM 3.1" en la página 9
- "Asistencia técnica y accesibilidad" en la página 10

Documentación relacionada

Documentación	Vínculos
Todos los productos de Oracle	http://www.oracle.com/documentation
Biblioteca de documentación de Oracle Integrated Lights Out Manager (ILOM) 3.1	http://www.oracle.com/pls/topic/lookup?ctx=ilom31
Documentación de gestión de sistemas, seguridad de gestión de sistema único (SSM) y diagnóstico	http://www.oracle.com/technetwork/documentation/sys-mgmt-networking-190072.html
Paquete de administración de hardware de Oracle 2.2	http://www.oracle.com/pls/topic/lookup?ctx=ohmp

Nota: Para ubicar la documentación de Oracle ILOM 3.1 específica para su plataforma de servidor Sun, consulte la sección Oracle ILOM de la guía de administración que está disponible para su servidor.

Comentarios sobre este documento

Puede ofrecernos sus comentarios sobre esta documentación en:

`http://www.oracle.com/goto/docfeedback`

Descargas de producto

Encontrará actualizaciones del firmware de Oracle ILOM 3.1 en las actualizaciones de software independientes que puede descargar del sitio web My Oracle Support (MOS) para cada servidor de Sun o sistema de chasis Sun Blade. Para descargar estas actualizaciones de software del sitio web MOS, consulte las instrucciones siguientes.

▼ Descarga de firmware y software de productos

1. **Vaya a `http://support.oracle.com`.**

2. **Inicie sesión en My Oracle Support.**

3. **En la parte superior de la página, haga clic en la ficha Patches & Updates (Parches y actualizaciones).**

4. **En el panel Patch Search (Búsqueda de parches), en la parte superior de la ficha Search (Buscar), seleccione Product or Family (Advanced Search) (Producto o familia [búsqueda avanzada]).**

5. **En el cuadro de lista Product Is? (¿Cuál es el producto?), escriba un nombre de producto parcial o completo hasta que aparezca una lista de coincidencia de productos en el cuadro de lista y, a continuación, seleccione el nombre de producto deseado.**

   Nombres de productos de ejemplo: Sun Fire X4470 M2 Server o Sun Enterprise SPARC T5120.

6. **En el cuadro de lista Release Is? (¿Cuál es la versión?):**

   a. **En el cuadro de lista Release Is? (¿Cuál es la versión?), haga clic en la flecha hacia abajo para mostrar una lista de carpetas de productos coincidentes.**

      Aparece una lista de uno o varios íconos de carpetas de productos.

   b. **Haga clic en el triángulo (>) junto al ícono de carpeta de productos para mostrar una lista de versiones de software.**

   c. **Seleccione la versión de software deseada.**

      Por ejemplo: `X4470 M2 SW 1.4` o `Sun SPARC Enterprise T5120`

7 **Haga clic en Search (Buscar).**

Aparece la pantalla Patch Search Results (Resultados de la búsqueda de parches), que muestra una lista de nombres de parches con sus respectivas descripciones.

8 **En la pantalla Patch Search Results (Resultados de la búsqueda de parches), seleccione el nombre de parche deseado.**

Por ejemplo: `X4470 M2 Server SW 1.4. ILOM and BIOS (Patch)` o `Firmware SPARC Enterprise T5120 Sun System Firmware 7.1.3.2`

9 **En la selección de nombres de parches, haga clic en una de las siguientes acciones:**

- **Readme (Léame): abre el archivo Readme (Léame) del parche seleccionado.**
- **Add to Plan (Agregar al plan): agrega el parche seleccionado a un plan nuevo o existente.**
- **Download (Descargar): descarga el parche seleccionado.**
- **Copy (Copiar): copia los detalles del parche seleccionado en la memoria.**

Esquema de numeración de versiones de firmware de Oracle ILOM 3.1

Oracle ILOM 3.1 utiliza un esquema de numeración de versiones de firmware que facilita la identificación de la versión de firmware que está ejecutando en su servidor o en el módulo de supervisión del chasis (CMM). El esquema de numeración incluye una cadena de cinco campos; por ejemplo, `a.b.c.d.e`, donde:

- `a` representa la versión principal de Oracle ILOM.
- `b` representa una versión menor de Oracle ILOM.
- `c` representa la versión de actualización de Oracle ILOM.
- `d` representa una microversión de Oracle ILOM. Las microversiones se gestionan por plataforma o grupo de plataformas. Consulte la documentación de la plataforma para obtener más información.
- `e` representa una nanoversión de Oracle ILOM. Las nanoversiones son iteraciones incrementales de una microversión.

Por ejemplo, Oracle ILOM 3.1.2.1.a representaría lo siguiente:

- Oracle ILOM 3 como versión principal
- Oracle ILOM 3.1 como versión menor
- Oracle ILOM 3.1.2 como segunda versión de actualización
- Oracle ILOM 3.1.2.1 como microversión

- Oracle ILOM 3.1.2.1.a como nanoversión de Oracle ILOM 3.1.2.1

Consejo – Para identificar la versión de firmware de Oracle ILOM instalada en el servidor Sun o en el CMM, haga clic en System Information (Información del sistema) > Firmware, en la interfaz web, o bien escriba `version` en la interfaz de la línea de comandos.

Asistencia técnica y accesibilidad

Descripción	Vínculos

Acceda a la asistencia técnica electrónica por medio de Internet en My Oracle Support	`http://support.oracle.com`
	Para personas con discapacidad auditiva:
	`http://www.oracle.com/accessibility/support.html`

Obtenga más información sobre el compromiso de Oracle para facilitar la accesibilidad	`http://www.oracle.com/us/corporate/accessibility/index.html`

Configuración de una conexión de gestión a Oracle ILOM e inicio de sesión

Descripción	Vínculos
Consulte esta sección para obtener información sobre las opciones de conexión de gestión admitidas a Oracle ILOM.	■ "Establecimiento de una conexión de gestión a Oracle ILOM" en la página 11
Consulte esta sección para obtener información sobre el inicio de sesión en Oracle ILOM, las cuentas de usuario preconfiguradas y los sistemas operativos y exploradores web admitidos.	■ "Inicio de sesión en el SP o en el CMM del servidor" en la página 30
Consulte esta sección para obtener información sobre cómo ubicar las directrices para mejorar la seguridad de Oracle ILOM.	■ "Configuración de Oracle ILOM para máxima seguridad" en la página 36

Información relacionada

- Guía de instalación para servidores Oracle o CMM de sistemas blade
- Guía de administración para servidores Oracle
- *Guía de seguridad de Oracle Integrated Lights Out Manager (ILOM) 3.1*

Establecimiento de una conexión de gestión a Oracle ILOM

El firmware Oracle ILOM se entrega preconfigurado en su servidor o módulo de supervisión del chasis (CMM) de Oracle de manera que simplifica el establecimiento de una conexión de gestión a Oracle ILOM.

Para obtener más información sobre cómo establecer una conexión de gestión a Oracle ILOM, consulte:

- "Selección y configuración de una conexión de gestión a Oracle ILOM" en la página 12
- "Servicios de gestión y propiedades predeterminadas de red" en la página 27

Selección y configuración de una conexión de gestión a Oracle ILOM

Oracle ILOM admite las siguientes conexiones de gestión:

- "Conexión de gestión de red dedicada (predeterminado)" en la página 12
- "Conexión de gestión de red de banda lateral" en la página 15
- "Conexión de gestión local dedicada" en la página 17
- "Conexión de gestión de SP de interconexión dedicada" en la página 18

Conexión de gestión de red dedicada (predeterminado)

Todos los CMM y servidores de Oracle suministrados con Oracle ILOM ofrecen un puerto de gestión en banda dedicado en el chasis que segrega, de manera segura, todo el tráfico de gestión fuera del host.

Todos los servidores y CMM se entregan listos para establecer una conexión de gestión segura a Oracle ILOM. Simplemente conecte una conexión LAN activa al puerto de gestión de red física (NET MGT) en el chasis y podrá iniciar sesión. Para obtener más instrucciones sobre cómo configurar una conexión de gestión dedicada a Oracle ILOM, consulte el siguiente procedimiento.

▼ Configuración de una conexión de gestión de red dedicada a Oracle ILOM

Antes de empezar

- Revise "Servicios de gestión y propiedades predeterminadas de red" en la página 27.
- La propiedad Management Port (Puerto de gestión) en Oracle ILOM está establecida, de forma predeterminada, para enrutar todo el tráfico de gestión a través del puerto de gestión de red física (NET MGT) en el dispositivo gestionado.

  Nota – La conexión de gestión de red dedicada está diseñada para implementarse de manera independiente a una conexión de gestión de red de banda lateral. No obstante, cualquiera de estas conexiones de red (dedicada o de banda lateral) puede coexistir con la conexión de gestión serie local estándar y (o) la conexión de gestión de interconexión de alta velocidad interna.

- La propiedad Management Port para Oracle ILOM se puede configurar desde la interfaz web y la CLI de Oracle ILOM. También se puede configurar para servidores x86, desde la utilidad del BIOS.

Si modifica la propiedad Management Port desde Oracle ILOM, debe iniciar sesión con la cuenta `root` predeterminada o una cuenta de usuario con privilegios de rol Admin (a). Para obtener instrucciones sobre el inicio de sesión, consulte "Inicio de sesión en el SP o CMM de Oracle ILOM" en la página 30.

Para verificar o configurar una conexión de gestión de red dedicada a Oracle ILOM, siga estos pasos:

1 **En el CMM o el servidor físico, verifique que se haya establecido una conexión LAN al puerto de gestión físico (NET MGT).**

Si no se ha establecido una conexión LAN física al puerto NET MGT, conecte un cable Ethernet entre el conmutador de red y el puerto físico NET MGT del dispositivo. Para obtener más instrucciones, consulte la sección de cableado en la guía de instalación del CMM o servidor de Oracle.

Nota – Cuando se conecta una conexión LAN activa al puerto NET MGT del servidor gestionado o chasis del CMM, Oracle ILOM automáticamente detecta una dirección IP para el SP o CMM desde el dispositivo de enrutamiento IP de la red. Para obtener directrices para determinar la dirección IP asignada al SP o CM de Oracle ILOM, consulte "Directrices de uso para la dirección de gestión de red IP" en la página 32.

---

2 **Para verificar que la propiedad Management Port predeterminada esté definida para el SP o CMM de Oracle ILOM, realice los siguientes pasos mediante la interfaz de usuario aplicable.**

<table>
<tr><th>Interfaz de usuario</th><th>Paso</th><th>Tarea: verificar o restablecer la propiedad de puerto de gestión predeterminada para SP o CMM</th></tr>
<tr><td rowspan="3">CLI de Oracle ILOM</td><td>1:</td><td>Inicie sesión en la CLI de Oracle ILOM y utilice el comando <code>show</code> para ver las propiedades de red del dispositivo gestionado, por ejemplo, escriba cualquiera de los siguientes comandos:
■ <code>show /SP/network</code>
■ <code>show /CMM/network</code>

Para obtener instrucciones sobre el inicio de sesión, consulte “Inicio de sesión en el SP o CMM de Oracle ILOM” en la página 30.</td></tr>
<tr><td>2:</td><td>Verifique que la salida de <code>/network</code> muestre la propiedad Management Port predeterminada del SP o CMM, por ejemplo:
■ Salida de SP: <code>managementport=MGMT</code>
■ Salida de CMM: <code>switchconf=port0</code></td></tr>
<tr><td>3:</td><td>En caso de que sea necesario, restablezca la propiedad Management Port predeterminada del SP o CMM.

Para el SP, escriba:

<code>set /SP/network pendingmanagementport=MGMT commitpending=true</code>

Para el CMM, escriba:

<code>set /CMM/network pendingswitchconf=port0 commitpending=true</code></td></tr>
<tr><td rowspan="2">Interfaz web de Oracle ILOM</td><td>1:</td><td>Inicie sesión en la interfaz web de Oracle ILOM y haga clic en ILOM Administration (Administración de ILOM) > Connectivity (Conectividad).

Para obtener instrucciones sobre el inicio de sesión, consulte “Inicio de sesión en el SP o CMM de Oracle ILOM” en la página 30.</td></tr>
<tr><td>2:</td><td>Si la página Network Settings (Configuración de red), verifique que el cuadro de lista Management Port del SP esté definido en <code>MGMT</code> o el cuadro de lista CMM Management Network Switch (Conmutador de red de gestión del CMM) esté definido en <code>Port 0</code>.

Si es necesario, restablezca la propiedad Management Port predeterminada seleccionando <code>MGMT</code> para SP o <code>Port0</code> para CMM y, a continuación, haga clic en Save (Guardar).</td></tr>
<tr><td rowspan="2">Utilidad de configuración del BIOS (disponible sólo para servidores x86)</td><td>1</td><td>Acceda a la utilidad de configuración del BIOS del servidor x86 gestionado; luego, en el cuadro de diálogo BIOS Setup Utility (Utilidad de configuración del BIOS), haga clic en Advanced (Avanzado) > IPMI 2.0 Configuration (Configuración de IPMI 2.0) > Set LAN Configuration (Establecer configuración de LAN).</td></tr>
<tr><td>2</td><td>En el menú LAN Configuration (Configuración de LAN), verifique que la propiedad Management Port predeterminada esté definida en <code>MGMT</code>.

Si es necesario, restablezca la propiedad Management Port predeterminada en <code>MGMT</code> y aplique el cambio.</td></tr>
</table>

Más información

Información relacionada

- “Modificación de las propiedades predeterminadas de configuración de la conectividad” en la página 107

- "Configuración y mantenimiento de cuentas de usuario" en la página 37

Conexión de gestión de red de banda lateral

Para los servidores que admiten gestión de banda lateral, puede conectarse, de manera opcional, a Oracle ILOM y gestionar el servidor de manera remota a través del puerto de datos estándar proporcionado en el chasis del servidor. La implementación de una conexión de gestión de banda lateral a Oracle ILOM elimina la necesidad de admitir dos conexiones de red separadas para el trafico de gestión y el host. Sin embargo, este enfoque puede: (1) disminuir potencialmente el rendimiento de la conexión a Oracle ILOM, y (2) presentar riesgos potenciales por transmitir el tráfico de Oracle ILOM a través de una red no confiable.

Para configurar Oracle ILOM de manera que transmita el tráfico de gestión a través de una conexión de gestión de banda lateral, debe cambiar el valor de propiedad Management Port (Puerto de gestión) predeterminado (`MGMT|port0`) al puerto de datos activo físico (`NET0`, `NET1`, `NET2` o `NET3`) en el servidor.

Para obtener más información sobre cómo configurar una conexión de gestión de banda lateral a Oracle ILOM, consulte lo siguiente:

- "Configuración de una conexión de gestión de banda lateral a Oracle ILOM" en la página 15
- "Consideraciones sobre la conectividad de red de gestión de banda lateral" en la página 17

▼ Configuración de una conexión de gestión de banda lateral a Oracle ILOM

Antes de empezar

- La gestión de banda lateral se admite en la mayoría de los servidores de Oracle. Sin embargo, para verificar si un servidor admite la gestión de banda lateral, consulte la guía de administración del servidor o las notas de versión del producto.

Nota – La conexión de gestión de red de banda lateral está diseñada para implementarse de manera independiente a una conexión de gestión de red dedicada. No obstante, cualquiera de estas conexiones de red (dedicada o de banda lateral) puede coexistir con la conexión de gestión serie local estándar y (o) la conexión de gestión de interconexión de alta velocidad interna.

- Revise "Servicios de gestión y propiedades predeterminadas de red" en la página 27.
- La propiedad SP Management Port (Puerto de gestión del SP) para Oracle ILOM se puede configurar desde la interfaz web y la CLI de Oracle ILOM. También se puede configurar para servidores x86, desde la utilidad de configuración del BIOS.

  Si modifica la propiedad Management Port (Puerto de gestión) a través de Oracle ILOM, se aplican los siguientes requisitos:

- Ya se debe haber establecido una conexión de gestión a Oracle ILOM. Para obtener instrucciones, consulte:

  - "Conexión de gestión de red dedicada (predeterminado)" en la página 12

  - "Conexión de gestión local dedicada" en la página 17

- Ya debe haber iniciado sesión en Oracle ILOM. Para obtener instrucciones, consulte "Inicio de sesión en el SP o en el CMM del servidor" en la página 30.
- Se requiere la cuenta `root` predeterminada o una cuenta de usuario con privilegios de rol Admin (a) en Oracle ILOM para modificar la propiedad Management Port.

Para configurar una conexión de gestión de banda lateral a Oracle ILOM, siga estos pasos:

1 **En el servidor físico, verifique que exista una conexión LAN activa al puerto de datos Ethernet correspondiente (`NET0`, `NET1`, `NET2` o `NET3`).**

Para obtener instrucciones, consulte la sección de cableado en la guía de instalación del servidor o sistema blade.

2 **Para configurar la propiedad SP Management Port para gestión de banda lateral, realice una de las siguientes acciones:**

- **Desde la interfaz web de Oracle ILOM: haga clic en ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) y luego en el cuadro de lista Management Port.**

  En el cuadro de lista Management Port, seleccione el nombre del puerto de datos físico activo (`NET0`, `NET1`, `NET2` o `NET3`) y haga clic en Save (Guardar).

- **Desde la CLI de Oracle ILOM: escriba:**

  `set /SP/network pendingmanagementport=/SYS/MB/NET`*`n`* `commitpending=true`

  Donde:

  n es el número de puerto de datos físico activo (0, 1, 2 o 3) del servidor.

- **Desde la utilidad de configuración del BIOS (disponible para servidores x86): haga clic en Advanced (Avanzado) > IPMI 2.0 Configuration (Configuración de IPMI 2.0) > Set LAN Configuration (Establecer configuración de LAN).**

  En el menú LAN Configuration, defina el valor Management Port en el nombre del puerto de datos físico activo (`NET0`, `NET1`, `NET2` o `NET3`); a continuación, haga clic en Commit (Confirmar) para aplicar el cambio.

  Nota – Para obtener información sobre cómo navegar, definir y guardar opciones en la utilidad de configuración del BIOS, consulte la guía de administración suministrada para el servidor.

Más información

Información relacionada

- "Consideraciones sobre la conectividad de red de gestión de banda lateral" en la página 17
- "Directrices de uso para la dirección de gestión de red IP" en la página 32
- "Modificación de las propiedades predeterminadas de configuración de la conectividad" en la página 107
- "Práctica recomendada para configuraciones de árbol de expansión " en la página 127
- "Configuración y mantenimiento de cuentas de usuario" en la página 37
- "Asignación de la información sobre identificación del sistema" en la página 121

Consideraciones sobre la conectividad de red de gestión de banda lateral

En esta sección, se proporcionan cuestiones generales de conectividad de red para que las tenga en consideración al usar una conexión de gestión de banda lateral a Oracle ILOM:

- Es posible que el controlador Gigabit Ethernet de host integrado no admita la conectividad en chip entre el SP del servidor y el sistema operativo del host. Si se produce esta situación, utilice un puerto diferente o ruta para transmitir el tráfico entre la fuente y el destino en lugar de utilizar la creación de puentes/conmutación L2.
- Apagar y volver a encender el host del servidor puede producir una breve interrupción de la conectividad de red en los puertos Gigabit Ethernet del servidor (`NET 0`, `1`, `2`, `3`) que se han configurado para la gestión de banda lateral. Si se produce esta situación, configure los puertos de conmutación/puente adyacentes como puertos del host.
- Si los puertos de datos Ethernet del servidor se configuran como puertos de conmutación y participan en el protocolo de árbol de expansión (STP), es posible que se produzcan interrupciones mayores por motivos de recálculo del árbol de expansión.

Conexión de gestión local dedicada

Todos los CMM y servidores de Oracle se entregan con un puerto serie físico en el chasis que facilita establecer una conexión de gestión local segura a Oracle ILOM. Este tipo de conexión de gestión resulta de especial utilidad cuando una consola local es la única forma de acceder y diagnosticar errores del sistema o cuando necesita un método alternativo para modificar las propiedades de red preconfiguradas de Oracle ILOM antes de establecer la conexión LAN.

Para obtener más información sobre cómo configurar una conexión de gestión serie local a Oracle ILOM, consulte lo siguiente:

▼ Configuración de una conexión de gestión local dedicada a Oracle ILOM

Antes de empezar

- Una conexión de gestión serie local a Oracle ILOM requiere conectar un dispositivo de consola serie físico (terminal de texto, estación de trabajo, equipo portátil o programa de emulación de terminal) al puerto SER MGT del servidor o CMM.

Para configurar una conexión de gestión local dedicada a Oracle ILOM, siga estos pasos:

1 **Conecte un cable serie entre el dispositivo de consola serie y el puerto de gestión serie (SER MGT) del servidor o CMM.**

2 **Defina las propiedades de comunicación de dispositivo de consola en estos valores: 9600 baudios, 8 bits, sin paridad, 1 bit de parada.**

Nota – Si las señales de transmisión y de recepción están invertidas (cruzadas) para comunicaciones de DTE a DTE, se necesita una configuración de módem nulo. Utilice el cable de adaptador proporcionado con su sistema para establecer una conexión de módem nulo.

---

3 **Para crear una conexión entre el dispositivo de consola y el SP o CMM de Oracle ILOM, pulse Enter (Intro).**

Más información

Información relacionada

- "Servicios de gestión y propiedades predeterminadas de red" en la página 27
- "Modificación de las propiedades predeterminadas de configuración de la conectividad" en la página 107
- "Roles de usuario asignables de Oracle ILOM" en la página 40
- "Propietario del puerto de gestión serie" en la página 89
- "Asignación de la información sobre identificación del sistema" en la página 121

Conexión de gestión de SP de interconexión dedicada

Para servidores de Oracle que admiten una interfaz interna de Ethernet a través de USB, puede, de manera opcional, establecer una conexión de gestión LAN a Oracle ILOM desde un cliente de sistema operativo (SO) del host sin usar el puerto de gestión de red (NET MGT) del servidor.

Algunas de las ventajas que obtiene al implementar este tipo de conexión de gestión, son las siguientes:

- **Direcciones IP no enrutables preconfiguradas para facilitar la implementación**

  La configuración de interconexión local se presenta lista para la configuración automática mediante las direcciones IP no enrutables internas preconfiguradas para cada punto de conexión interno (SP de ILOM y SO del host).

  Oracle ILOM presenta la interfaz Ethernet a través de USB que está instalada en un servidor gestionado como una interfaz "Ethernet" estándar.

- **Una conexión local autenticada segura a Oracle ILOM**

  La conexión a Oracle ILOM a través de la interconexión local requiere autenticación del usuario como si se estableciera la conexión a Oracle ILOM a través de una conexión de gestión de red dedicada o de banda lateral.

  Todos los usuarios del sistema operativo con nombre de usuario y contraseña válidos pueden acceder a Oracle ILOM.

- **Una alternativa rápida para la gestión local**

  Realice todas las tareas de gestión de Oracle ILOM a través de una conexión de gestión dedicada de alta velocidad interna.

  Una conexión de gestión de interconexión local ofrece una alternativa para gestionar el servidor localmente más rápida que utilizar una consola serie local tradicional o una interfaz KCS (Keyboard Controller Style) del host.

Para obtener más información sobre cómo establecer una conexión de interconexión local al SP de Oracle ILOM, consulte estos temas:

- "Opciones de configuración para la interconexión local" en la página 19
- "Configuración manual de la interconexión local" en la página 20
- "Directrices de interconexión del SO del host para la conexión manual" en la página 23
- "Propiedades de interconexión del SP de Oracle ILOM " en la página 26

Opciones de configuración para la interconexión local

Opción de configuración de interconexión local	Descripción
Configuración automática (recomendada)	Oracle ILOM automatiza la configuración de la conexión de gestión de interconexión local al instalar el software Oracle Hardware Management Pack 2.1.0 o posterior. En este caso no es necesario realizar ninguna configuración desde Oracle ILOM. **Nota –** La configuración automática de los puntos de conexión de interconexión local requiere que el valor predeterminado `Host Managed` (host gestionado) (`hostmanaged`) en Oracle ILOM esté activado (establecido en `True`), así como que el software Oracle Hardware Management Pack 2.1.0 o posterior esté instalado en el servidor. Para obtener información sobre la configuración automática mediante Oracle Hardware Management Pack, consulte la *Guía del usuario de Oracle Hardware Management Pack* (E20451).
Configuración manual (Usuarios avanzados)	Si es un administrador de red avanzado y prefiere no configurar automáticamente los puntos de conexión Ethernet USB mediante la instalación de Oracle Hardware Management Pack, puede optar por configurar manualmente los puntos de conexión en la interfaz Ethernet USB interna. Para obtener información acerca de la configuración manual, consulte "Configuración manual de la interconexión local" en la página 20.

▼ Configuración manual de la interconexión local

Nota – De manera alternativa, puede utilizar el software Oracle Hardware Management Pack 2.1.0 o posterior para configurar automáticamente los puntos de conexión de interconexión local en un servidor gestionado. Para obtener instrucciones para la configuración automática de interconexión local, consulte la *Guía del usuario de Oracle Hardware Management Pack* (E20451).

Antes de empezar

- Revise "Opciones de configuración para la interconexión local" en la página 19.
- Este procedimiento manual para configurar una interconexión local entre el SP y el SO del host debe ser realizado sólo por usuarios avanzados.
- Este procedimiento manual ofrece directrices para configurar el punto de conexión interno del SO del host y los pasos detallados para configurar opcionalmente el punto de conexión interno del SP de Oracle ILOM.
- Se requiere una conexión de gestión serie local o de red establecida al SP de Oracle ILOM antes de modificar las propiedades predeterminadas de interconexión del host local del SP en Oracle ILOM.

Nota – La propiedad Local Host Interconnect (Interconexión del host local) en Oracle ILOM no está disponible para un CMM. No obstante, puede utilizar la interfaz web o la CLI del CMM de Oracle ILOM para navegar hasta las propiedades de interconexión del host local del SP y configurarlas para un servidor blade instalado en el chasis.

- Se necesita la cuenta `root` preconfigurada de Oracle ILOM o una cuenta de usuario configurada por el cliente con privilegios de rol Admin (`a`) para modificar las propiedades de interconexión del host local del SP en Oracle ILOM.

Siga estos pasos para configurar manualmente los puntos de conexión Ethernet USB internos entre el SO del host y el SP de Oracle ILOM:

1 Para configurar manualmente los parámetros de conexión Ethernet USB interna para el sistema operativo del host, realice lo siguiente:

a. Verifique que el servidor admita una interfaz Ethernet sobre USB interna.

Para verificar si un servidor admite una conexión de gestión de interconexión local a Oracle ILOM, consulte la sección que describe las funciones admitidas de Oracle ILOM en la guía de administración del servidor.

b. Asegúrese de que el controlador del dispositivo Ethernet específico del SO haya sido instalado por la distribución de software del SO en el servidor gestionado.

Si un controlador del dispositivo Ethernet específico del SO no se incluyó con su instalación del sistema operativo, puede obtenerlo para la interfaz Ethernet sobre USB interna de la distribución de software Oracle Hardware Management Pack 2.1.0 o posterior. Para obtener más información sobre cómo extraer este archivo de la distribución del software Oracle Hardware Management Pack, consulte la *Guía del usuario de Oracle Hardware Management Pack*.

c. Confirme que el sistema operativo del host del servidor gestionado reconoce la interfaz Ethernet sobre USB interna. A continuación, asigne manualmente los parámetros de red al punto de conexión del SO del host.

Para obtener directrices, consulte "Directrices de interconexión del SO del host para la conexión manual" en la página 23.

2 Para modificar manualmente las propiedades de interconexión del host local para el SP de Oracle ILOM, siga estos pasos:

a. Revise "Propiedades de interconexión del SP de Oracle ILOM " en la página 26.

b. Inicie sesión en Oracle ILOM mediante un explorador web o un shell de la CLI.

Para obtener instrucciones sobre el inicio de sesión, consulte "Inicio de sesión en el SP o en el CMM del servidor" en la página 30.

c. Para modificar las propiedades de interconexión del host local del SP en Oracle ILOM, realice los pasos siguientes para la interfaz correspondiente de Oracle ILOM.

Interfaz de Oracle ILOM	Paso:
Explorador web	a. En la interfaz web del SP de Oracle ILOM, haga clic en ILOM Administration (Administración de ILOM) > Connectivity (Conectividad). b. Desplácese por la página hasta la sección Local Host Interconnect (Interconexión del host local) y haga clic en Configure (Configurar). c. En el cuadro de diálogo Configure USB Ethernet Parameters (Configurar parámetros de Ethernet USB), borre la casilla de verificación correspondiente a Host Managed (Host gestionado) y, sólo si es necesario, modifique la dirección IPv4 no enrutable local o las direcciones de máscara de red proporcionadas para el SP y haga clic en Save (Guardar). **Nota**: No es necesario modificar la dirección IP preconfigurada o la dirección de máscara de red asignada al SP de Oracle ILOM, a menos que haya conflicto con estos parámetros en la red.

Interfaz de Oracle ILOM	Paso:
Shell de la CLI	a. Navegue hasta el directorio de trabajo `/network/interconnect` del servidor gestionado. **Por ejemplo:** Desde la CLI del SP, escriba: **`cd /SP/network/interconnect`** Desde la CLI del CMM, escriba: **`cd /Servers/Blades/BL`*n*`/network/interconnect`** b. Para desactivar la propiedad `hostmanaged` y establecer el estado de interconexión del host local en `true`, escriba lo siguiente: **`set hostmanaged=disabled`** **`set state=true`** **Nota**: No es necesario modificar la dirección IP no enrutable preconfigurada o la dirección de máscara de red asignada al SP de Oracle ILOM, a menos que haya conflicto con estos parámetros en la red. c. Para modificar la dirección IPv4 no enrutable local o la dirección de máscara de red suministrada para el SP, escriba lo siguiente: **`set pendingipaddress=`***specify_new_address* **`set pendingipnetmask=`***specify_new_address* **`set commitpending=true`**

3 **Para probar la conexión de gestión de interconexión local entre el SO del host y el SP de Oracle ILOM, realice cualquiera de las siguientes acciones:**

- **En el sistema operativo del host del servidor gestionado, mediante un explorador web o un shell de la CLI, inicie sesión en el SP de Oracle ILOM. Para ello, introduzca la dirección IP no enrutable asignada al punto de conexión Ethernet USB del SP.**

  Resultados esperados para:

  Conexión con explorador web: aparece la página de inicio de sesión de Oracle ILOM.

  Conexión con shell de la CLI: aparece un indicador de autorización para Oracle ILOM.

- **Haga ping en la dirección de interconexión local del SP desde el SO del host.**

  Para obtener instrucciones, consulte “Prueba de la conectividad de IPv4 e IPv6” en la página 128.

Más información

Información relacionada

- “Directrices de interconexión del SO del host para la conexión manual” en la página 23
- “Propiedades de interconexión del SP de Oracle ILOM ” en la página 26
- “Inicio de sesión en el SP o en el CMM del servidor” en la página 30
- *Guía de seguridad de Oracle Integrated Lights Out Manager (ILOM) 3.1*, Descripción de la interfaz de interconexión LAN
- Biblioteca de documentos de Oracle Hardware Management Pack en: `http://www.oracle.com/pls/topic/lookup?ctx=ohmp`

Directrices de interconexión del SO del host para la conexión manual

La siguiente tabla proporciona directrices generales para configurar los parámetros de la red local para el puerto de conexión Ethernet USB interno del SO del host.

Nota – El dispositivo Ethernet USB interno instalado en el servidor gestionado se presenta en el sistema como una interfaz Ethernet tradicional. Al configurar manualmente el punto de interconexión local para el SO del host, es posible que sea necesario usar la dirección MAC del host (`hostmacaddress=`) a fin de determinar el nombre asignado al punto de interconexión local del SO del host.

TABLA 1 Directrices para la configuración manual de la interconexión del SO del host

Sistema operativo	Directrices para la interconexión manual del SO del host
Windows Server 2008	Después de que Microsoft Windows detecta la interfaz Ethernet sobre USB interna en el servidor gestionado, es posible que se muestre un mensaje que le indique identificar un controlador de dispositivo para la interfaz Ethernet sobre USB. Dado que en realidad no se precisa ningún controlador, la identificación del archivo `.inf`, el cual se extrae de la distribución del software Oracle Hardware Management Pack, debería satisfacer la pila de comunicación para la interfaz Ethernet sobre USB. La distribución del software Oracle Hardware Management Pack 2.1.0 o posterior está disponible para descarga desde la página de descargas de productos de software de Oracle. Para obtener información sobre la extracción del archivo `.inf` de Oracle Server Hardware Management Pack, consulte la *Guía del usuario de Oracle Server Hardware Management Pack* (E24501). Para obtener más información que describa cómo configurar los parámetros de la red IP en Windows Server 2008, consulte la documentación del sistema operativo Microsoft Windows o el siguiente sitio Microsoft Tech Net: `http://technet.microsoft.com/en-us/library/cc754203%28WS.10%29.aspx`

TABLA 1 Directrices para la configuración manual de la interconexión del SO del host *(Continuación)*

Sistema operativo	Directrices para la interconexión manual del SO del host

Linux	La mayoría de las instalaciones de sistemas operativos Linux compatibles en un servidor gestionado incluyen la instalación del controlador de dispositivo para la interfaz Ethernet sobre USB interna.
	
	Por lo general, la interfaz Ethernet sobre USB es detectada automáticamente por el sistema operativo Linux y se presenta en el sistema como `usb0`. No obstante, el nombre presentado para esta interfaz puede variar según una distribución de software Linux específica.
	
	Las siguientes instrucciones de línea de comandos demuestran cómo configurar los parámetros de red para la conexión de interconexión del SO del host correspondiente a `usb0`:
	
	`\>lsusb usb0`
	
	`\> ifconfig usb0 169.254.182.77`
	
	`\> ifconfig usb0 netmask 255.255.255.0`
	
	`\> ifconfig usb0 broadcast 169.254.182.255`
	
	`\> ifconfig usb0`
	
	`\> ip addr show usb0`
	
	Nota – En lugar de ejecutar comandos `ifconfig` individuales, puede generar secuencias de comandos para la configuración de parámetros de la red. No obstante, la secuencia de comandos de red exacta para configurar los parámetros de red pueden variar entre cada distribución de software Linux. Por lo tanto, debe consultar los ejemplos de secuencias de comandos de la red que generalmente se suministran con cada distribución del software Linux.
	
	Para obtener más información sobre cómo configurar los parámetros de la red IP mediante un sistema operativo Linux, consulte la documentación del sistema operativo Linux.

TABLA 1 Directrices para la configuración manual de la interconexión del SO del host *(Continuación)*

<table>
<tr><th>Sistema operativo</th><th>Directrices para la interconexión manual del SO del host</th></tr>
<tr><td>Solaris</td><td>
La mayoría de las instalaciones de sistemas operativos Oracle Solaris en un servidor gestionado incluyen el controlador de dispositivo para la interfaz Ethernet sobre USB. Si no se suministra el controlador de dispositivo para esta interfaz, puede extraerlo de la distribución del software Oracle Hardware Management Pack 2.1.0 o posterior.
Para obtener información sobre cómo extraer el controlador de SO específico de Solaris del paquete de gestión, consulte la Guía del usuario de Oracle Hardware Management Pack (E20451).
Por lo general, la interfaz Ethernet sobre USB es detectada automáticamente por el sistema operativo Oracle Solaris y se presenta en el sistema como <code>usbecm0</code>. No obstante, el nombre presentado para esta interfaz puede variar según la distribución de software Oracle Solaris.
Las siguientes instrucciones de línea de comandos demuestran cómo configurar los parámetros de red para la conexión de interconexión del SO del host correspondiente a <code>usbecm0</code>:

Escriba el siguiente comando para asociar (<code>plumb</code>) la interfaz IP o disociar (<code>unplumb</code>) la interfaz IP:
<code>ifconfig usbecm0 plumb</code>
<code>ifconfig usbecm0 unplumb</code>
Escriba los siguientes comandos para establecer la información de la dirección:
<code>ifconfig usbecm0 netmask 255.255.255.0 broadcast 169.254.182.255 169.254.182.77</code>
Para configurar la interfaz, escriba:
<code>ifconfig usbecm0 up</code>
Para cancelar la interfaz, escriba:
<code>ifconfig usbecm0 down</code>
Para mostrar la interfaces activas, escriba:
<code>ifconfig -a</code>
Para probar la conectividad, haga ping en el host Oracle Solaris o en el dispositivo USB Ethernet interno del SP.
<code>ping</code> <<i>IPv4 address of Oracle Solaris host</i>>
<code>ping</code> <I<i>Pv4 address of SP-Ethernet-over- USB interface</i>>

Nota – En lugar de ejecutar los pasos de <code>ifconfig</code>, puede generar secuencias de comandos para la configuración de parámetros de la red. No obstante, la secuencia de comandos de red exacta para configurar los parámetros de red pueden variar entre cada distribución de software Oracle Solaris. Por lo tanto, debe consultar los ejemplos de secuencias de comandos de la red que generalmente se suministran con cada distribución del software Oracle Solaris.
Para obtener más información sobre cómo configurar una dirección IP estática para un dispositivo de hardware que utiliza el sistema operativo Oracle Solaris, consulte la documentación del sistema operativo Oracle Solaris.
</td></tr>
</table>

Propiedades de interconexión del SP de Oracle ILOM

La siguiente tabla describe las propiedades de interconexión del host local del SP que se muestran en la CLI de Oracle Solaris (destino: `/network/interconnect`) y la interfaz web de Oracle ILOM (ILOM Administration [Administración de ILOM] > Connectivity [Conectividad] > Local Host Interconnect [Interconexión del host local] >Configure [Configurar]).

TABLA 2 Propiedades de interconexión del SP de Oracle ILOM

Propiedad	Valor predeterminado	Descripción
Host Managed (Host gestionado) (`hostmanaged=`*true*|*false*)	Enabled (Activado) (`true`)	La propiedad Host Managed, se entrega lista, de forma predeterminada, para que el software Oracle Hardware Management Pack configure automáticamente la conexión de gestión de interconexión local entre el SO del host y el SP de Oracle ILOM. Para impedir que el software Oracle Hardware Management Pack configure automáticamente la conexión de interconexión local o para configurar manualmente los puntos de conexión entre el SO del host y el SP de Oracle ILOM, el valor de la propiedad Host Managed debe establecerse en desactivado (`false`). **Nota**: Para impedir el uso de la interfaz Ethernet sobre USB, tanto la propiedad Host Managed como la propiedad del estado Local Host Interconnect (Interconexión del host local) deben estar desactivadas (`false`) en Oracle ILOM.
State `(Estado)` (`state=`*disabled*|*enabled*)	`Disabled` (Desactivado)	El estado de la propiedad de interconexión del host local en Oracle ILOM está establecido en desactivado de forma predeterminada. Si elige configurar manualmente los puntos de conexión Ethernet sobre USB entre el SO del host y el SP de Oracle ILOM, el valor de esta propiedad debe estar establecido en activado.
IP Address (Dirección IP) (`pendingipaddress=`)	`169.254.182.7`	De forma predeterminada, Oracle ILOM ofrece una dirección IPv4 no enrutable preconfigurada para el punto de conexión Ethernet sobre USB del SP de Oracle ILOM. Por lo general, no necesitará modificar la dirección IP preconfigurada (169.254.182.76), a menos que exista conflicto con esta dirección en la red.
Netmask Address (Dirección de máscara de red) (`pendingipnetmask=`)	`255.255.255.0`	De forma predeterminada, Oracle ILOM ofrece una dirección de máscara de red IPv4 preconfigurada para el punto de conexión Ethernet sobre USB del SP de Oracle ILOM. Por lo general, no necesitará modificar la dirección de máscara de red IPv4 preconfigurada (255.255.255.0), a menos que exista conflicto con esta dirección en la red.

TABLA 2 Propiedades de interconexión del SP de Oracle ILOM *(Continuación)*

Propiedad	Valor predeterminado	Descripción
Save (Guardar) (`commitpending=`*true*|*false*)		Todas las modificaciones que se realicen a la dirección IP o dirección de máscara de red para el punto de conexión Ethernet sobre USB del SP de Oracle ILOM se consideran pendientes hasta que los cambios se confirmen en la CLI o se guarden en la interfaz web.
Service Processor MAC Address (Dirección MAC del procesador de servicio) (`spmacaddress=`)	Read-only (Sólo lectura)	La propiedad de sólo lectura de la dirección MAC del procesador de servicio muestra la dirección MAC asignada al SP de Oracle ILOM.
Host MAC Address (Dirección MAC del host) (`hostmacaddress=`)	Read-only	La propiedad de sólo lectura de la dirección MAC del host muestra la dirección MAC asignada al servidor gestionado y también representa la forma en que la mayoría de los sistemas operativos reconocen la interfaz Ethernet sobre USB interna.
Connection Type (Tipo de conexión)	Read-only	La propiedad Connection Type (Tipo de conexión) de sólo lectura indica el tipo conexión como Ethernet USB interna.
Comando `help` de la CLI		Para obtener más información sobre las propiedades configurables y no configurables que se muestran en el destino `/network/interconnect` de la CLI, puede escribir el comando `help` seguido del nombre de la propiedad. *Sintaxis:* **`help`** /*SP*|*CMM***`/network/interconnect`** *property_name* *Ejemplo:* **`help /SP/network/interconnect hostmanaged`**

Servicios de gestión y propiedades predeterminadas de red

Para ayudar a simplificar el proceso de implementación de un servidor, Oracle ILOM se entrega preconfigurado con la mayoría de los puertos de servicio de gestión y propiedades de conectividad de red estándar activados. No obstante, para maximizar la seguridad e impedir el acceso no autorizado a Oracle ILOM, debe desactivar las propiedades de los puertos de servicio de gestión que no sean necesarios.

Nota – Las propiedades predeterminadas en Oracle ILOM pueden ser configuradas por el usuario después de establecer una conexión de gestión a Oracle ILOM.

- Tabla 3
- Tabla 4

TABLA 3 Servicios de gestión activados de forma predeterminada

Acceso de gestión	Propiedades predeterminadas	Puerto de servicio	Para modificar las propiedades configurables, consulte:
Servidor web: Modo	■ Redirección de conexión HTTP a HTTPS	80	Tabla 35
Servidor web: Estado	■ HTTPS, activado	443	Tabla 35
Servidor web: SSL	■ SSLv3 y TLSv1 activados ■ Certificado SSL predeterminado ■ Clave privada de autofirma de SSL predeterminada	-	Tabla 36
IPMI: Estado	■ Enabled	623	Tabla 39
SNMP: Estado	■ SNMPv3, Enabled	161	Tabla 37
WS-MAN: Modo	■ HTTP, Enabled	8889	Tabla 41
Inicio de sesión único	■ Enabled	11626	"Servicio de inicio de sesión único (activado de forma predeterminada)" en la página 42
Shell seguro (SSH)	■ Enabled ■ Generación de claves de RSA y DSA	22	Tabla 38
Redirección de KVMS remoto (video, teclado, mouse y almacenamiento)	■ Enabled	5120-5123, 5555, 5556, 7578, 7579	"Uso de consolas de KVMS remoto para la redirección de servidores host" en la página 129
Etiqueta de servicio[1]	■ Enabled	6481	Para modificar la propiedad Service Tag (Etiqueta de servicio), escriba: **set /SP/services/servicetag state=***enabled*|*disabled*

[1] Protocolo de detección de Oracle que identifica servidores y proporciona integración con soluciones de servicios de Oracle.

Nota – Para obtener una lista completa de los puertos de red predeterminados utilizados por Oracle ILOM, consulte "Puertos de red predeterminados utilizados por Oracle ILOM" en la página 89.

TABLA 4 Propiedades de conectividad de red activadas de forma predeterminada

Propiedad de conectividad de red	Valor predeterminado	Para modificar las propiedades configurables, consulte:
Network: State (Red: Estado)	■ Enabled	Tabla 43
IPv4: Mode (Modo)	■ DHCP, enabled	
IPv6: State (Estado)	■ Enabled	Tabla 43
IPv6: Mode (Modo)	■ Auto-Config, Stateless (Configuración automática, sin estado)	
Management Port (Puerto de gestión):	■ Dedicated Network Management (Gestión de red dedicada) (MGMT)	Tabla 43
Local Host Interconnect (Interconexión del host local)	■ Host Utilities Managed (Utilidades de host gestionadas): Enabled ■ State: Disabled	"Conexión de gestión de SP de interconexión dedicada" en la página 18
DNS	■ Auto DNS via DHCP, Enabled (DNS automático por medio de DHCP, activado)	Tabla 44
Serial Port (Puerto serie)	■ Owner (Propietario): Service Processor (Procesador de servicio) ■ Baud Rate (Velocidad en baudios): 9600 ■ Host Flow Control (Control de flujo de host): None	Tabla 45
User Authentication (Autenticación de usuario)[1]	■ Root user account (Cuenta de usuario root) root ■ Root password (Contraseña root): `changeme` ■ Permitted local accounts (Cuentas locales permitidas): Hasta 10 cuentas de usuario configurables por el usuario ■ Single Sign On: Activado para KVMS remoto y navegación de blade de CMM (Detalle).	"Gestión de credenciales de usuario " en la página 38

[1] Los estados de propiedad para LDAP, RADIUS y Active Directory están desactivados, de forma predeterminada.

Inicio de sesión en el SP o en el CMM del servidor

Oracle ILOM incluye parámetros de red predeterminados y cuenta de usuario preconfigurada que simplifica el inicio de sesión en Oracle ILOM por primera vez. Para obtener más información sobre el inicio de sesión en Oracle ILOM, consulte estos temas:

- "Inicio de sesión en el SP o CMM de Oracle ILOM" en la página 30
- "Directrices de uso para la dirección de gestión de red IP" en la página 32
- "Cuentas de usuario preconfiguradas activadas de forma predeterminada" en la página 33
- "Exploradores web de sistemas operativos compatibles" en la página 35

▼ Inicio de sesión en el SP o CMM de Oracle ILOM

Antes de empezar

- Se requiere una conexión de gestión local o de red establecida a Oracle ILOM.

  Para obtener instrucciones, consulte "Selección y configuración de una conexión de gestión a Oracle ILOM" en la página 12.
- Se requiere la cuenta `root` preconfigurada de Oracle ILOM o una cuenta de usuario configurada por el usuario para iniciar sesión en Oracle ILOM.

  Para obtener información sobre la cuenta `root` preconfigurada, consulte "Cuentas de usuario preconfiguradas activadas de forma predeterminada" en la página 33. Para obtener información sobre cómo crear cuentas de usuario en Oracle ILOM, consulte "Gestión de credenciales de usuario " en la página 38.

Para iniciar sesión en Oracle ILOM desde una conexión de gestión serie local o una conexión de gestión de red, siga estos pasos:

1 Para iniciar sesión en Oracle ILOM, realice los siguientes pasos para la interfaz de Oracle ILOM correspondiente:

Interfaz de Oracle ILOM	Pasos
Consola serie local (puerto SER MGT)	■ Después de crear una conexión entre la consola y Oracle ILOM pulsando Enter (Intro), escriba el nombre de usuario y la contraseña de Oracle ILOM cuando se le solicite. Por ejemplo: Escriba `root` para nombre de usuario y `changeme` para contraseña.

Interfaz de Oracle ILOM	Pasos
Explorador web	a. Escriba **http://***ILOM_SP_or_CMM_ipaddress* en el explorador web y pulse Enter (Intro). Aparece la página de inicio de sesión en Oracle ILOM. Para obtener directrices para introducir la dirección IP asignada a Oracle ILOM, consulte "Directrices de uso para la dirección de gestión de red IP" en la página 32. b. Inicie sesión en la interfaz web de Oracle ILOM especificando un nombre de usuario y una contraseña válidos para Oracle ILOM. Por ejemplo: Escriba `root` para nombre de usuario y `changeme` para contraseña. Aparece la página Summary (Resumen) de Oracle ILOM.
Shell seguro de la CLI	a. Para establecer una sesión SSH con la CLI de Oracle ILOM, abra una ventana de terminal. b. Para iniciar sesión en Oracle ILOM con la cuenta `root` predeterminada, escriba: $ **ssh root@***ILOM_SP_or_CMM_ipaddress* Oracle ILOM le solicitará la contraseña `root`. c. Cuando aparezca el indicador de la contraseña, escriba `changeme`. Aparece el símbolo de sistema de Oracle ILOM (`->`).

2 Para salir de Oracle ILOM, realice una de las siguientes acciones:

- **Para salir de la sesión de la interfaz web de Oracle ILOM: haga clic en el botón Log Out (Cerrar sesión) ubicado en la parte superior derecha de la página de la interfaz web.**
- **Para salir de la sesión de la CLI de Oracle ILOM CLI: escriba: `exit (salir)`**

Más información

Información relacionada

- "Asignación de la información sobre identificación del sistema" en la página 121
- "Tiempo de espera predeterminado para sesiones web y de la CLI" en la página 88
- "Modificación de las propiedades predeterminadas de configuración de acceso de gestión" en la página 92
- "Visualización de mensajes de rótulo en el inicio de sesión" en la página 88
- "Configuración y mantenimiento de cuentas de usuario" en la página 37
- "Recuperación de contraseñas para la cuenta `root`" en la página 45
- "Configuración de una conexión de gestión a Oracle ILOM e inicio de sesión" en la página 11
- "Uso de consolas de KVMS remoto para la redirección de servidores host" en la página 129
- *User?s Guide*, Collecting System Information, Monitoring Health Status, and Initiating Host Management
- *User?s Guide*, Mapping Management Tasks to CLI Namespace Targets

- "Ejecución de actualizaciones de firmware" en la página 201

Directrices de uso para la dirección de gestión de red IP

La siguiente tabla proporciona directrices para ayudar a determinar: (1) la dirección IP asignada al SP o CMM de Oracle ILOM en función de las propiedades de red predeterminadas, (2) la sintaxis aceptada de iPv6 y 3) una lista de servidores IPv6 no compatibles.

TABLA 5 Identificación de dirección IP, sintaxis aceptada de IPv6 y servidores IPv6 no compatibles

Para determinar:	Directrices
Dirección IP asignada a Oracle ILOM	Para determinar la dirección IP asignada, realice estos pasos. 1. Establezca una conexión de gestión serie local (SER MGT) al SP o CMM de ILOM. 2. Inicie sesión en Oracle ILOM 3. Utilice el comando `show` para ver las propiedades de la red IP en: `/SP/network` para la dirección IPv4 actual asignada a Oracle ILOM. `/SP/networkipv6` para la dirección IPv6 actual asignada a Oracle ILOM. También puede determinar la dirección IP del servidor DHCP IPv4 o el dispositivo de enrutamiento IPv6 en la red.
Sintaxis aceptada para la dirección de red IPv6	■ Al introducir la URL en un explorador web, la dirección IPv6 *debe estar entre* corchetes para que funcione correctamente. Por ejemplo: **`https://[`***ipv6address***`]`** ■ Al establecer una sesión de la CLI de Oracle ILOM mediante SSH, la dirección IPv6 *no debe estar entre* corchetes. Por ejemplo: **`ssh root@`***ipv6address* ■ Al transferir un archivo mediante el comando `load -source` de la CLI y `tftp`, la dirección IPv6 *debe estar entre* corchetes. Por ejemplo: **`load -source tftp://[`***ipv6address***`]`***filename.extension*

TABLA 5 Identificación de dirección IP, sintaxis aceptada de IPv6 y servidores IPv6 no compatibles *(Continuación)*

Para determinar:	Directrices	
Servidores Sun heredados no compatibles con IPv6	Servidores Sun SPARC	■ T5440 ■ T5220 ■ T5120 ■ T5140 ■ T5240 ■ T6340
	Servidores Sun Fire:	■ X4140 ■ X4150 ■ X4240 ■ X4440 ■ X4450 ■ X4600 ■ X4600 M2 ■ X4640

Cuentas de usuario preconfiguradas activadas de forma predeterminada

Oracle ILOM incluye una cuenta de usuario administrador preconfigurada conocida como `root,` y una cuenta de usuario de recuperación de contraseña conocida como `default`. Para obtener más información acerca del uso de estas cuentas, consulte la siguiente tabla.

TABLA 6 Cuentas de usuario locales activadas de forma predeterminada

Cuenta de usuario preconfigurada	Propiedades de inicio de sesión predeterminadas	Descripción	Pa modificar, consulte:
`root`	■ Nombre de usuario: `root` ■ Contraseña: `changeme`	La cuenta de usuario `root` de Oracle ILOM es una cuenta de usuario local persistente que está disponible en todas las interfaces de Oracle ILOM[1], a menos que elija eliminar la cuenta de usuario `root` persistente. **Privilegios administrativos incorporados**: la cuenta `root` incluye privilegios administrativos incorporados (lectura y escritura) para todas las características, funciones y comandos de ILOM. **Práctica de seguridad recomendada**: para impedir el acceso no autorizado al servidor gestionado o CMM, debe: ■ Modificar la contraseña `root` predeterminada (`changeme`) suministrada en cada procesador de servicio (SP) o el módulo de supervisión del chasis (CMM) de Oracle ILOM. O bien: ■ Eliminar la cuenta `root` preconfigurada suministrada en el SP o CMM de Oracle ILOM. Antes de eliminar la cuenta `root` predeterminada, debe reemplazar la cuenta `root` por una cuenta de usuario local configurada por el cliente o un servicio de directorio como LDAP o Active Directory. **Nota.** Cuando la contraseña de la cuenta `root` se establece en `changeme` (contraseña predeterminada), aparece un mensaje de advertencia en la CLI al momento del inicio de sesión y aparece un mensaje de advertencia en la parte superior de la página de la interfaz web.	"Gestión de credenciales de usuario " en la página 38

[1] Interfaz web de Oracle ILOM, shell de la CLI, consola serie local e IPMI.

TABLA 6 Cuentas de usuario locales activadas de forma predeterminada *(Continuación)*

Cuenta de usuario preconfigurada	Propiedades de inicio de sesión predeterminadas	Descripción	Pa modificar, consulte:
valor predeterminado	■ `Username (Nombre de usuario): default` (predet.) ■ `Password (Contraseña): defaultpassword`	La cuenta de usuario `default` preconfigurada suministrada en Oracle ILOM está limitada a la recuperación de contraseña. **Uso de consola serie local solamente**: la cuenta de usuario `default` preconfigurada está disponible para ser utilizada a través de una conexión serie local solamente. Asimismo, debe ser capaz de probar la presencia física en el servidor o CMM. **Escenario de uso**: si elimina la cuenta `root` en Oracle ILOM antes de reemplazar la cuenta root por una cuenta configurable por el usuario, puede utilizar la cuenta `default` para iniciar sesión en Oracle y usar los comandos normales de Oracle ILOM para crear una cuenta nueva. **Información relacionada**: ■ Tabla 12 ■ (Presencia física) “Asignación de la información sobre identificación del sistema” en la página 121	“Recuperación de contraseñas para la cuenta `root`” en la página 45

Exploradores web de sistemas operativos compatibles

Oracle ILOM admite los siguientes exploradores web de sistemas operativos.

Nota – Para obtener una lista de sistemas operativos compatibles con el servidor gestionado, consulte la guía de administración o las notas del producto del servidor.

TABLA 7 Exploradores web de sistemas operativos compatibles

Sistema operativo	Explorador web
Oracle Solaris 10	■ Mozilla 1.4 y 1.7 ■ Firefox 3.6.x y 6
Linux (Oracle, Red Hat, SuSE, Ubuntu 10.10)	■ Firefox 3.6.x y 6
Microsoft Windows (XP Service Pack 2, Windows 7)	■ Internet Explorer 7.x, 8.x (para Windows XP Service Pack 2) y 9 (para Windows 7) ■ Firefox 3.6.x y 6
Macintosh (OSX v10.6 y posterior)	■ Firefox 3.6.x y 6 ■ Safari (todas)

Configuración de Oracle ILOM para máxima seguridad

Todas las propiedades configurables en Oracle ILOM pueden desactivarse o activarse de manera opcional para que el entorno de gestión de Oracle ILOM sea más seguro. Para obtener más información acerca de cómo mejorar la seguridad en Oracle ILOM, consulte las directrices de seguridad descritas en la *Guía de seguridad de Oracle ILOM 3.1*.

Configuración y mantenimiento de cuentas de usuario

Descripción	Vínculos
Consulte esta sección para conocer las opciones de configuración de la autenticación, los privilegios de los roles de usuario, el servicio de inicio de sesión único, las sesiones de usuario permitidas, la configuración de claves SSH, o la recuperación de cuentas y contraseñas `root` preconfiguradas.	■ "Gestión de credenciales de usuario " en la página 38
Consulte esta sección para conocer los requisitos y las instrucciones para configurar cuentas de usuario locales en Oracle ILOM.	■ "Configuración de cuentas de usuario locales " en la página 46
Consulte esta sección para conocer los requisitos y las instrucciones para configurar Oracle ILOM como cliente de Active Directory.	■ "Configuración de Active Directory " en la página 49
Consulte estas secciones para conocer los requisitos y las instrucciones para configurar Oracle ILOM como cliente LDAP/SSL o cliente LDAP.	■ "Configuración de LDAP/SSL" en la página 62 ■ "Configuración de LDAP" en la página 74
Consulte esta sección para conocer los requisitos y las instrucciones para configurar Oracle ILOM como cliente RADIUS.	■ "Configuración de RADIUS " en la página 78

Información relacionada

- *SNMP, IPMI, CIM, WS-MAN Protocol Management*, Manage User Accounts Using SNMP
- *Guía de seguridad de Oracle ILOM 3.1*, Seguridad de Oracle ILOM durante la implementación
- "Cuentas de usuario preconfiguradas activadas de forma predeterminada" en la página 33

Gestión de credenciales de usuario

El acceso de los usuarios a Oracle ILOM se controla mediante cuentas de usuario autenticadas. La autorización para usar funciones discretas dentro de Oracle ILOM se gestiona a través de un conjunto de roles de usuario asignados a una cuenta de usuario de Oracle ILOM.

Al configurar las credenciales de usuario en Oracle ILOM por primera vez, los administradores del sistema pueden optar por configurar hasta 10 cuentas de usuario locales o configurar un servicio de autenticación centralizado para permitir cuentas de usuario adicionales.

Para obtener más detalles sobre las opciones de configuración admitidas para las credenciales de usuario en Oracle ILOM, además de detalles generales sobre cómo gestionar credenciales de usuario en Oracle ILOM, consulte los siguientes temas:

- "Opciones de configuración admitidas para la autenticación de usuarios" en la página 38
- "Roles de usuario asignables de Oracle ILOM" en la página 40
- "Servicio de inicio de sesión único (activado de forma predeterminada)" en la página 42
- "Número máximo de sesiones de usuario admitidas" en la página 43
- "Sesiones de usuario autenticadas visibles por dispositivo gestionado" en la página 43
- "Autenticación de CLI con clave SSH de usuario local " en la página 44
- "Recuperación de contraseñas para la cuenta `root`" en la página 45
- "Métodos de transferencia de archivos admitidos" en la página 45

Opciones de configuración admitidas para la autenticación de usuarios

Antes de elegir y configurar cómo desea implementar la autenticación de usuarios en Oracle ILOM, tenga en cuenta la siguiente información.

TABLA 8 Opciones de configuración para la autenticación de usuarios

<table>
<tr><th>Opción</th><th colspan="2">Características y consideraciones</th></tr>
<tr><td>Local User Account Authentication (Autenticación de cuentas de usuario locales)</td><td colspan="2">■ Hasta 10 cuentas de usuario configurables almacenadas de manera local en Oracle ILOM.
■ Se incluyen dos cuentas de usuario preconfiguradas para una implementación y mantenimiento rápidos: cuenta de usuario `root` y cuenta de usuario `default` (consulte “Cuentas de usuario preconfiguradas activadas de forma predeterminada” en la página 33).
■ Privilegios de roles de usuario configurables que otorgan acceso de sólo lectura o de lectura y escritura a funciones discretas de Oracle ILOM (consulte “Roles de usuario asignables de Oracle ILOM” en la página 40).
■ Autenticación y autorización segura de usuarios para gestión local y remota.
■ Las credenciales de usuario de Oracle ILOM se mantienen por separado para cada SP y CMM.

Para obtener información adicional sobre cómo configurar cuentas de usuario locales en Oracle ILOM, consulte “Configuración de cuentas de usuario locales ” en la página 46.</td></tr>
<tr><td rowspan="4">Authentication Directory Service (Servicio de directorio de autenticación)</td><td colspan="2">■ Proporciona a los usuarios acceso a Oracle ILOM con más de 10 cuentas de usuario locales.
■ Permite que los administradores del sistema creen y mantengan credenciales de usuario de manera centralizada para todas las instancias de Oracle ILOM (todos los CMM y SP de servidor gestionados en el entorno de red local).
■ Permite que los usuarios autenticados de Oracle ILOM tengan acceso a todas las instancias de Oracle ILOM.
■ Permite que los administradores del sistema configuren reglas de autenticación de usuarios para utilizar las funciones dentro de Oracle ILOM.</td></tr>
<tr><td colspan="2">Supported Authentication Services (Servicios de autenticación admitidos)</td></tr>
<tr><td>Active Directory</td><td>Active Directory es un servicio distribuido que se incluye con los sistemas operativos Windows Server de Microsoft. El servicio de Active Directory es seguro de forma predeterminada.

Para obtener información adicional sobre cómo configurar Oracle ILOM para utilizar el servicio de autenticación de Active Directory, consulte “Configuración de Active Directory ” en la página 49.</td></tr>
<tr><td>LDAP/SSL</td><td>El servicio de autenticación LDAP/SSL es seguro de forma predeterminada. Admite un modo de certificado estricto opcional que requiere el uso de un certificado de seguridad.

Para obtener información adicional sobre cómo configurar Oracle ILOM como cliente LDAP/SSL, consulte “Configuración de LDAP/SSL” en la página 62.</td></tr>
</table>

TABLA 8 Opciones de configuración para la autenticación de usuarios *(Continuación)*

Opción	Características y consideraciones	
	LDAP	El servicio de autenticación LDAP (v2) es menos seguro que LDAP/SSL. Configure este servicio sólo si comprende y acepta las limitaciones de seguridad. Para obtener información adicional sobre cómo configurar Oracle ILOM como cliente LDAP, consulte "Configuración de LDAP" en la página 74.
	RADIUS	El servicio de autenticación remota telefónica de usuario (RADIUS) es un protocolo de red que utiliza un modelo de cliente/servidor para permitir la autenticación y autorización de usuarios. Para obtener información adicional sobre cómo configurar Oracle ILOM para utilizar el servicio de autenticación RADIUS, consulte "Configuración de RADIUS " en la página 78.

Roles de usuario asignables de Oracle ILOM

Durante la creación de cuentas de usuario de Oracle ILOM, un administrador del sistema asigna un conjunto de privilegios que otorgan a los usuarios acceso a funciones y operaciones discretas dentro de Oracle ILOM. Estos privilegios en Oracle ILOM se conocen como *roles de usuario*.

Oracle ILOM proporciona hasta seis roles de usuario predefinidos. Un administrador del sistema puede asignar roles para otorgar privilegios a un usuario o revocar privilegios de él.

Además de los roles de usuario, Oracle ILOM proporciona perfiles de usuario conocidos como Administrator (Administrador), Operator (Operador) y Advanced Roles (Roles avanzados). Estos perfiles de usuario permiten que un administrador del sistema asigne varios privilegios a la vez a un único usuario.

Un administrador del sistema puede utilizar el perfil Administrator u Operator para asignar un conjunto de roles de usuario predefinidos a una única cuenta de usuario. O bien, un administrador del sistema puede configurar el perfil Advanced Roles para asignar cualquiera de los seis roles de usuario predefinidos a una única cuenta.

Todos los privilegios de usuario se pueden asignar a una cuenta de usuario desde la interfaz web o la CLI. Para obtener una descripción de los privilegios otorgados por un único perfil o un rol de usuario, consulte las siguientes tablas:

- Tabla 9
- Tabla 10

TABLA 9 Privilegios otorgados por un perfil de usuario

Propiedad de web	Propiedad de CLI	Privilegios otorgados por perfil
Administrador (Administrador)	administrator	El perfil Administrator (`administrator`) viene predefinido con los siguientes roles de usuario: ■ Admin (a) ■ User Management (u) ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) Para obtener una descripción de los privilegios otorgados por cada rol de usuario, consulte la Tabla 10.
Operator (Operador)	operator	El perfil Operator (`operator`) viene predefinido con los siguientes roles de usuario: ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) Para obtener una descripción de los privilegios otorgados por cada rol de usuario, consulte la Tabla 10.
Advanced Roles (Roles avanzados)	*a|u|c|r|o|s*	La opción de perfil Advanced Roles es una opción que el usuario puede configurar únicamente desde la interfaz web. La opción de perfil Advanced Roles permite que los administradores del sistema asignen cualquiera de los siguientes seis roles de usuario a una única cuenta de usuario: ■ Admin (a) ■ User Management (u) ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) ■ Service (s) **Nota –** Los mismos seis roles de usuario (*a|u|c|r|o|s*) pueden asignarse de manera individual a una única cuenta de usuario desde la CLI. Para obtener una descripción de los privilegios otorgados por cada rol de usuario, consulte la Tabla 10.

TABLA 10 Privilegios otorgados por roles de usuario individuales

Rol de usuario	Privilegios otorgados
Admin (Administrador) (a)	El rol de usuario Admin (`a`), cuando está activado, otorga permisos de lectura y escritura para todas las funciones de gestión del sistema de Oracle ILOM, con excepción de las funciones que requieren que el rol Admin (a) tenga activados estos roles de usuario adicionales: User Management (`u`), Reset and Host Control (`r`), Console (`c`) y Service (`s`).

TABLA 10 Privilegios otorgados por roles de usuario individuales *(Continuación)*

Rol de usuario	Privilegios otorgados
User Management (Gestión de usuarios) (`u`)	El rol de usuario User Management (`u`), cuando está activado, otorga permisos de lectura y escritura a todas las funciones de autenticación para la gestión de usuarios de Oracle ILOM.
Console (Consola) (`c`)	El rol de usuario Console (`c`), cuando está activado, otorga permisos de lectura y escritura para realizar estas funciones de gestión de la consola remota: opciones de bloqueo de la consola remota, opciones de registro de historial de la consola del SP, inicio y uso de Oracle ILOM Remote Console, e inicio y uso de Oracle ILOM Storage Redirection CLI.
Reset and Host Control (Restablecimiento y control del host) (`r`)	El rol de usuario Reset and Host Control (`r`), cuando está activado, otorga permisos de lectura y escritura para realizar estas funciones de gestión del host: control de dispositivos de inicio del host, ejecución y configuración de utilidades de diagnóstico, reinicio del SP, reinicio del CMM, acciones de servicio técnico de subcomponentes, acciones de gestión de fallos, acciones de gestión de TMP de SPARC y operación de descarga de MIB de SNMP.
Read-Only (Sólo lectura) (`o`)	El rol de usuario Read-Only (`o`) otorga permisos de sólo lectura para ver el estado de todas las propiedades de configuración de Oracle ILOM y para cambiar las propiedades de contraseña de la cuenta y tiempo de espera de la sesión que están asignadas a la cuenta de usuario individual.
Service (Servicio) (`s`)	El rol de usuario Service (`s`), cuando está activado, otorga permisos de lectura y escritura para ayudar a los ingenieros del servicio de asistencia de Oracle en caso de que sea necesario realizar una reparación in situ.
`a|u|c|r|o`	La combinación de todos estos roles de usuario (`aucro`), cuando está activada, otorga permisos de lectura y escritura para realizar funciones de configuración de copia de seguridad y restauración en Oracle ILOM.

Servicio de inicio de sesión único (activado de forma predeterminada)

La función de inicio de sesión único (SSO, Single Sign-On) de Oracle ILOM es un servicio de protocolo propiedad de Oracle que permite que:

- Los usuarios autenticados de la interfaz web del SP de Oracle ILOM inicien las aplicaciones KVMS (Oracle ILOM Remote Console u Oracle ILOM Storage Redirection CLI), sin necesidad de volver a escribir sus contraseñas.
- Los usuarios autenticados de la interfaz web del CMM de Oracle ILOM naveguen a los servidores blade gestionados que están instalados en el chasis, sin necesidad de volver a escribir sus contraseñas.

El estado de la propiedad del servicio SSO está activado de forma predeterminada en Oracle ILOM. Para modificar el estado de esta propiedad, consulte la siguiente tabla.

Destino configurable de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**services/**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > User Accounts (Cuentas de usuario) > Single Sign On (Inicio de sesión único)
- **Rol de usuario:** Admin (a) (requerido para la modificación de propiedades)

Propiedad	Valor predeterminado	Descripción
Single Sign On (Inicio de sesión único) (/sso state=)	Enabled (Activado)	*Enabled* |*Disabled* **Sintaxis de la CLI para estado de SSO:** **set /***SP*|*CMM***/services/sso state=***enabled*|*disabled*

Número máximo de sesiones de usuario admitidas

Oracle ILOM admite un máximo de 10 sesiones de usuario activas por cada CMM o SP de servidor gestionado. Algunos sistemas SPARC están limitados a un máximo de 5 sesiones de usuario activas por cada SP de servidor gestionado.

Nota – Se considera una *sesión de usuario activa* cualquiera de las siguientes conexiones con Oracle ILOM: consola serie, shell seguro (SSH) o interfaz web.

Sesiones de usuario autenticadas visibles por dispositivo gestionado

Los administradores del sistema pueden identificar una lista de los usuarios que están conectados de forma activa con un SP o CMM de Oracle ILOM mediante la CLI o la interfaz web. Para ver una lista de las sesiones de usuario para una única instancia de SP o CMM, consulte la siguiente tabla.

Destino configurable de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**services/**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Sessions (Sesiones activas)
- **Rol de usuario:** perfil Administrator (administrator) (aucro)

Propiedad	Descripción
Active Sessions (Sesiones activas) (sessions)	La información de sesiones activas, para un único SP o CMM, enumera las sesiones de usuario autenticadas que actualmente están conectadas con Oracle ILOM. **Sintaxis de la CLI para sesiones activas**: ■ **show /***SP*|*CMM***/sessions** ■ **show /***SP*|*CMM***/sessions***n*

Autenticación de CLI con clave SSH de usuario local

Como alternativa al uso de una contraseña de usuario estándar, los administradores del sistema pueden asociar un archivo de clave SSH pública generado con una cuenta de usuario para obtener acceso a la CLI de Oracle ILOM a través de un shell seguro. Al asociar un archivo de clave SSH pública generado con una cuenta de Oracle ILOM, las secuencias de comandos automatizadas pueden ejecutar comandos del SP en Oracle ILOM de manera segura, sin ninguna intervención manual o sin necesidad de insertar una contraseña de texto no cifrado.

Antes de anexar un archivo de clave SSH pública con una cuenta de usuario de Oracle ILOM, primero debe generar el par de clave privada y clave pública con una herramienta de conectividad de SSH, como ssh-keygen, y almacenar los archivos de clave SSH generados en un sistema SSH remoto.

Para cargar y anexar un archivo de clave SSH pública generado en una cuenta de usuario de Oracle ILOM o para quitar un archivo de clave SSH pública de usuario de una cuenta de usuario de Oracle ILOM, consulte la siguiente tabla.

TABLA 11 Adición o eliminación de un archivo de clave SSH pública por cuenta de usuario local

Destino configurable de la interfaz de usuario:

- **CLI:** `/`*SP*`|`*CMM*`/services/`
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > User Accounts (Cuentas de usuario) > SSH Key (Clave SSH)
- **Rol de usuario:** Read-Only (o) para clave SSH personal, User Management (u) para otra clave SSH de usuario

Propiedad	Descripción
Key Upload - File Transfer Options (Carga de claves - Opciones de transferencia de archivos) (`set load_uri=`)	*Browser*|*TFTP*|*SFTP*|*SCP*|*HTTP*|*HTTPS*|*Paste* Para obtener una descripción de cada método de transferencia de archivos, consulte la Tabla 13.
Add SSH Key (Agregar clave SSH) (`/ssh/keys/1`)	Sintaxis de la CLI para agregar clave SSH: **`set /SP/users/`***user_account_name***`/ssh/keys/1`** **`load_uri=`***transfer_method://username:password@ipaddress_or_hostname/directorypath/filename* **Ejemplo:** set /SP/users/adminuser/ssh/keys/1 load_uri=scp://adminuser:userpswd@1.2.3.4/keys/sshkey_1.pub
Delete SSH Key (Suprimir clave SSH) (clear action=true)	**Sintaxis de la CLI para suprimir clave SSH**: **`set /`***SP*|*CMM***`/users/`***user_account_name***`/ssh/keys/1 clear_action=true`** Escriba **`y`** para borrar la clave SSH pública o escriba **`n`** para cancelar la operación.
Save (Guardar)	**Interfaz web únicamente**. Para aplicar los cambios realizados en las propiedades dentro del cuadro de diálogo SSH Key (Clave SSH), debe hacer clic en Save (Guardar).

Recuperación de contraseñas para la cuenta `root`

Si es necesario, los administradores del sistema pueden recuperar la cuenta root local preconfigurada de Oracle ILOM o la contraseña de la cuenta `root` local mediante la contraseña predeterminada preconfigurada de Oracle ILOM. Para obtener instrucciones de recuperación adicionales, consulte la siguiente tabla.

TABLA 12 Recuperación de cuenta `root` preconfigurada o contraseña de cuenta `root` (sólo CLI)

Requisitos previos	Instrucciones

■ Conexión de gestión serie local con Oracle ILOM
■ Presencia física en el servidor gestionado, si Physical Presence State (Estado de presencia física) está activado (predeterminado)
	1. Establezca una conexión de gestión serie local con ILOM e inicie sesión en ILOM mediante la cuenta de usuario predeterminada. Por ejemplo:
	`SUNSP-0000000000 login: default Press and release the physical presence button.`
	`Press return when this is completed...`
	2. Compruebe la presencia física en el servidor.
	Consulte la documentación de hardware del servidor para obtener instrucciones sobre cómo comprobar la presencia física.
	3. Vuelva a la consola serie y pulse Intro.
	Se le solicitará una contraseña.
	4. Escriba la contraseña de la cuenta de usuario predeterminada: `defaultpassword`.
	5. Restablezca la contraseña de la cuenta o vuelva a crear la cuenta root.
	Consulte la sección Información relacionada de esta tabla si desea conocer los temas para crear o modificar cuentas de usuario o contraseñas.
	Información relacionada
	■ “Configuración de una conexión de gestión local dedicada a Oracle ILOM” en la página 17
	■ (Presencia física) “Asignación de la información sobre identificación del sistema” en la página 121
	■ Tabla 14
	■ Tabla 15

Métodos de transferencia de archivos admitidos

Oracle ILOM admite los siguientes métodos de transferencia para cargar archivos, como claves SSH o certificados de seguridad.

TABLA 13 Métodos de transferencia de archivos

Método de transferencia de archivos	Descripción
Browser (Explorador)	El método de transferencia de archivos Browser sólo está disponible para la interfaz web. Este método permite seleccionar un archivo que está almacenado de manera local en el sistema o de forma remota en un recurso compartido de red.
TFTP	El método de transferencia de archivos TFTP requiere que se especifique el nombre del host de TFTP y la ruta del directorio para cargar el archivo designado en Oracle ILOM.
FTP	El método de transferencia de archivos FTP requiere que se especifique el nombre del sistema host de FTP, el nombre de usuario y la contraseña del host de FTP y la ruta del directorio para cargar el archivo designado.
SFTP	El método de transferencia de archivos SFTP requiere que se especifique el nombre del sistema host de SFTP, el nombre de usuario y la contraseña del host de SFTP y la ruta del directorio del archivo designado.
SCP	El método de transferencia de archivos SCP requiere que se especifique el nombre del sistema host de SCP, el nombre de usuario y la contraseña del host de SCP y la ruta del directorio del archivo designado.
HTTP	El método de transferencia de archivos HTTP requiere que se especifique el nombre del sistema host de HTTP, el nombre de usuario y la contraseña de HTTP y la ruta del directorio del archivo designado.
HTTPS	El método de transferencia de archivos HTTPS requiere que se especifique el nombre del sistema host de HTTPS, el nombre de usuario y la contraseña del host de HTTPS y la ruta del directorio del archivo designado.
Paste (Pegar)	El método de transferencia de archivos Paste sólo está disponible para la interfaz web. Este método proporciona un cuadro de texto para pegar en el archivo de certificado personalizado.

Configuración de cuentas de usuario locales

Los administradores del sistema pueden crear y mantener hasta 10 cuentas de usuario locales en Oracle ILOM. Para obtener instrucciones sobre cómo usar las propiedades configurables en Oracle ILOM para crear o mantener cuentas de usuario locales, consulte las siguientes tablas:

- Tabla 14
- Tabla 15

TABLA 14 Creación de cuenta de usuario y asignación de roles de usuario

Destino configurable de la interfaz de usuario:

- **CLI:** */SP*|*CMM*/users/
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > User Accounts (Cuentas de usuario)
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)

Propiedad	Descripción
Users (Usuarios) > Add (Agregar) (*user_name* password= role =)	*user_name* |Password=|Role=*administrator* |*operator*|*advanced* (a|u|c|r|o|s) Complete las propiedades que se muestran en Add User (Agregar usuario) con un nombre de usuario y una contraseña, confirme la contraseña y asigne un rol de usuario. El nombre de usuario debe tener entre 4 y 16 caracteres, debe comenzar con un carácter alfabético y no debe incluir espacios. La contraseña debe tener entre 8 y 16 caracteres, los cuales distinguen mayúsculas de minúsculas. Utilice cualquier carácter, excepto dos puntos y espacios. **Sintaxis de la CLI para crear usuario**: **create** */SP*|*CMM*/**users/***user_name_for_account* **password=** *password_for_account* **role=***administrator*|*operator*|*a*|*u*|*c*|r|o|s **Ejemplo de sintaxis:** `create /SP/users user5 password=administrator role=aucr` **Nota**. Al agregar una cuenta de usuario a través de la CLI, no es necesario proporcionar un valor de propiedad para un rol o una contraseña. El rol tendrá el valor predeterminado Read-Only (o), y la CLI solicitará que se proporcione y confirme una contraseña.
Save (Guardar)	**Interfaz web**. Para aplicar los cambios realizados en las propiedades dentro del cuadro de diálogo Add User (Agregar usuario), debe hacer clic en Save (Guardar).
	Información relacionada: ■ Tabla 9 ■ Tabla 15 ■ Tabla 6 ■ Tabla 12 ■ "Autenticación de CLI con clave SSH de usuario local" en la página 44

TABLA 15 Visualización, modificación o eliminación de cuenta de usuario

Destino configurable de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**users/**
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > User Accounts (Cuentas de usuario)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**

Propiedad	Descripción
Users (Usuarios) (/users)	Permite ver las cuentas de usuario locales configuradas en Oracle ILOM. **Sintaxis de la CLI para ver usuarios**: **show** /*SP*|*CMM*/**users** **Ejemplo de sintaxis:** `show /SP/users`
Users (Usuarios) > Edit (Editar) (/*user_name* password= role=)	Password=*user_configurable*|role=*administrator* |*operator*|*advanced* (a|u|c|r|o|s) Permite editar las propiedades de usuario aplicables para la contraseña y el rol de usuario. La contraseña debe tener entre 8 y 16 caracteres, los cuales distinguen mayúsculas de minúsculas. Utilice cualquier carácter, excepto dos puntos y espacios. Tenga en cuenta que los roles de usuario no se pueden modificar para el usuario root preconfigurado. **Interfaz web**. Haga clic en Save (Guardar) para aplicar los cambios realizados dentro del cuadro de diálogo Edit User (Editar usuario). **Sintaxis de la CLI para editar cuenta de usuario**: **set** /*SP*|*CMM*/**users** *user_name* **password=***assign_new_password* **role=***administrator*|*operator*|*a*|*u*|*c*|r|o|s **Ejemplo de sintaxis**: `set /SP/users user5 password=administrator role=auco`
Users (Usuarios) > Delete (Suprimir) (/*user_name*)	Especifique el nombre de la cuenta de usuario que desea suprimir. Cuando se le solicite, confirme la acción. **Sintaxis de la CLI para suprimir cuenta de usuario:** **delete** /*SP*|*CMM*/**users**/*user_name* **Ejemplo de sintaxis:** `delete /SP/users/user5`
	Información relacionada: - Tabla 9 - Tabla 14 - Tabla 12

Configuración de Active Directory

De manera opcional, los administradores del sistema pueden configurar Oracle ILOM para utilizar el servicio de Active Directory de Microsoft Windows a fin de autenticar los usuarios de Oracle ILOM, así como definir los niveles de autorización de usuarios para las funciones dentro de Oracle ILOM. Este servicio está basado en un modelo de consulta de cliente/servidor que utiliza la contraseña de usuario asignada para autenticar usuarios de Active Directory.

La propiedad para el estado del servicio de Active Directory está desactivada de forma predeterminada en Oracle ILOM. Para activar el estado del servicio de Active Directory y configurar Oracle ILOM como cliente de Active Directory, consulte las siguientes tablas:

- Tabla 16
- Tabla 17
- Tabla 18
- Tabla 19
- Tabla 20
- Tabla 21
- Tabla 22

TABLA 16 Activación de la autenticación de Active Directory

Destino configurable de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**clients/activedirectory**
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Settings (Configuración)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo:** **se debe configurar el servidor de Active Directory con los usuarios o grupos de usuarios antes de configurar Oracle ILOM como cliente de Active Directory.**

Propiedad	Valor predeterminado	Descripción
State (Estado) (`state=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Para configurar Oracle ILOM como cliente de Active Directory, establezca el estado de la propiedad State en activado. Cuando se activa la propiedad State y se desactiva la propiedad Strict Certificate Mode (Modo de certificado estricto), Oracle ILOM proporciona a través de un canal seguro una validación limitada del certificado del servicio de Active Directory durante la autenticación de usuarios. Cuando se activa la propiedad State y también se activa la propiedad Strict Certificate Mode, Oracle ILOM realiza a través de un canal seguro una verificación completa de las firmas digitales del certificado del servicio de Active Directory durante la autenticación de usuarios. **Sintaxis de la CLI para estado**: **set /***SP*|*CMM***/clients/activedirectory/ state=***disabled***|***enabled*

TABLA 16 Activación de la autenticación de Active Directory *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/activedirectory**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Settings (Configuración)
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)
- **Requisito previo:** se debe configurar el servidor de Active Directory con los usuarios o grupos de usuarios antes de configurar Oracle ILOM como cliente de Active Directory.

Propiedad	Valor predeterminado	Descripción
Roles (`defaultrole=`)	None (server authorization) [Ninguno (autorización de servidor)]	*Administrator |Operator |Advanced |None (server authorization)* Para definir qué funciones de Oracle ILOM estarán disponibles para los usuarios autenticados de Active Directory, establezca la propiedad Roles predeterminada en uno de los cuatro valores de propiedad aceptados: Administrator (a|u|c|r|o), Operator (c|r|o), Advanced (*a*|*u*|*c*|*r*|*o*|*s*) o None (server authorization). Cuando se establece la propiedad Roles predeterminada en un rol de usuario de Oracle ILOM, los niveles de autorización para usar las funciones dentro de Oracle ILOM estarán determinados por los privilegios otorgados mediante el rol de usuario configurado de Oracle ILOM. Para obtener una descripción de los privilegios asignados, consulte los temas sobre roles de usuario y perfiles de usuario que se enumeran a continuación en la sección Información relacionada. Cuando se establece la propiedad Roles en `None (server authorization)` y se configura Oracle ILOM para utilizar los grupos de Active Directory, los niveles de autorización para usar las funciones dentro de Oracle ILOM estarán determinados por el grupo de Active Directory. Para obtener detalles adicionales sobre la configuración, consulte el tema sobre el grupo de Active Directory que se enumera a continuación en la sección Información relacionada. **Sintaxis de la CLI para roles**: **set /***SP*|*CMM***/clients/activedirectory/ defaultrole=***administrator*|*operator*|*a*|*u*|*c*|*r*|*o*|*s*|*none* **Información relacionada:** ■ Tabla 9 ■ Tabla 9 ■ Tabla 18

TABLA 16 Activación de la autenticación de Active Directory *(Continuación)*

Destino configurable de la interfaz de usuario:
- **CLI**: */SP*|*CMM*/**clients/activedirectory**
- **Web**: **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Settings (Configuración)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: se debe configurar el servidor de Active Directory con los usuarios o grupos de usuarios antes de configurar Oracle ILOM como cliente de Active Directory.**

Propiedad	Valor predeterminado	Descripción
Address (Dirección) (`address=`)	0.0.0.0	*IP address*| *DNS host name* (servidor de Active Directory) Para configurar la dirección de red del servidor de Active Directory, complete la propiedad Address con la dirección IP del servidor de Active Directory o el nombre de host DNS. Si se utiliza un nombre de host DNS, las propiedades de configuración de DNS deberán estar definidas y activadas correctamente en Oracle ILOM. **Sintaxis de la CLI para dirección**: **set /***SP*|*CMM***/clients/activedirectory/ address=***active_directory_server ip_address*|*active_directory_server_dns_host_name* **Información relacionada:** ■ Tabla 44
Port (Puerto) (`port=`)	0 Auto-select (Selección automática)	*0 Auto-select* | *Non-standard TCP port* Oracle ILOM utiliza un puerto TCP estándar para comunicarse con el servidor de Active Directory. Cuando se activa la propiedad Port: Auto-select, el número de puerto se establece en 0 de forma predeterminada. Cuando se desactiva la propiedad Port: Auto-select, el usuario puede configurar la propiedad de número de puerto de la interfaz web. Se proporciona una propiedad Port configurable en el caso poco probable de que Oracle ILOM necesite usar un puerto TCP no estándar. **Sintaxis de la CLI para puerto**: **set /***SP*|*CMM***/clients/activedirectory/ port=***number*
Timeout (Tiempo de espera) (`timeout=`)	4 segundos	*4* |*user-specified* La propiedad Timeout designa la cantidad de segundos que se debe esperar para que se complete una transacción individual. El valor no representa el tiempo total que tardan en completarse todas las transacciones, ya que la cantidad de transacciones puede variar según la configuración. La propiedad Timeout se establece en 4 segundos de forma predeterminada. Si es necesario, ajuste el valor de esta propiedad para optimizar el tiempo de respuesta para los casos en que el servidor de Active Directory no esté disponible o no responda. **Sintaxis de la CLI para tiempo de espera**: **set /***SP*|*CMM***/clients/activedirectory/ timeout=***number_of_seconds*

TABLA 16 Activación de la autenticación de Active Directory *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/activedirectory**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Settings (Configuración)
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)
- **Requisito previo:** se debe configurar el servidor de Active Directory con los usuarios o grupos de usuarios antes de configurar Oracle ILOM como cliente de Active Directory.

Propiedad	Valor predeterminado	Descripción
Strict Certificate Mode (Modo de certificado estricto) (`strictcertmode=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Cuando se activa la propiedad Strict Certificate Mode, Oracle ILOM realiza una verificación completa de las firmas digitales del certificado de Active Directory durante la autenticación. Cuando se desactiva la propiedad Strict Certificate Mode, Oracle ILOM proporciona una validación limitada del certificado del servidor durante la autenticación a través de un canal seguro. **Precaución –** El certificado del servidor de Active Directory se debe cargar antes de activar la propiedad Strict Certificate Mode. **Sintaxis de la CLI para modo de certificado estricto**: **set /***SP*|*CMM***/clients/activedirectory/ strictcertmode=***disabled***|***enabled* **Información relacionada**: ■ Tabla 17
DNS Locator Mode (Modo de localizador de DNS) (`/dnslocatorqueries`)	Disabled (Desactivado)	*Disabled* | *Enabled* Para configurar Oracle ILOM para usar las consultas del localizador de DNS a fin de obtener una lista de los servidores de Active Directory, establezca el estado de la propiedad DNS Locator Mode en activado. **Sintaxis de la CLI para modo de localizador de DNS**: **set /***SP*|*CMM***/clients/activedirectory/ dnslocatorqueries/1=***disabled***|***enabled* **Información relacionada**: ■ Tabla 21

TABLA 16 Activación de la autenticación de Active Directory *(Continuación)*

Destino configurable de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**clients/activedirectory**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Settings (Configuración)
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)
- **Requisito previo:** se debe configurar el servidor de Active Directory con los usuarios o grupos de usuarios antes de configurar Oracle ILOM como cliente de Active Directory.

Propiedad	Valor predeterminado	Descripción
Expanded Search Mode (Modo de búsqueda ampliada) (`expsearchmode=`)	Disabled (Desactivado)	*Enabled*|*Disabled* Para configurar Oracle ILOM para usar opciones de búsqueda adicionales a fin de localizar entradas de usuario de Active Directory, establezca el estado de la propiedad Expanded Search Mode en activado. Cuando se desactiva la propiedad Expanded Search Mode, Oracle ILOM utilizará userPrincipleName para buscar entradas de usuario. En este caso, userPrincipleName deberá tener un sufijo de nombre de dominio completo (FQDN). **Sintaxis de la CLI para modo de búsqueda ampliada**: **set /***SP*|*CMM***/clients/activedirectory/ expsearchmode=***disabled***|***enabled*
Strict Credential Error Mode (Modo de error de credenciales estricto) (`strictcredentialerrormode=`)	Disabled (Desactivado)	*Disabled* | *Enabled* Si se activa la propiedad Strict Credential Error Mode y se informan errores de credenciales de usuario en cualquier servidor, Oracle ILOM generará errores para esas credenciales de usuario. Si se desactiva la propiedad Strict Credential Error Mode, Oracle ILOM presentará las credenciales de usuario a otros servidores de Active Directory para la autenticación (configurados como servidores alternativos o detectados por las consultas del localizador de DNS). **Sintaxis de la CLI para configuración del modo de certificado estricto**: **set /***SP*|*CMM***/clients/activedirectory/ strictcredentialerrormode=***disabled***|***enabled* **Información relacionada**: ■ Tabla 17
Log Detail (Detalle de registro) (`logdetail=`)	None (Ninguno)	*None* | *High* | *Medium* | *Low* |*Trace* Para especificar la cantidad de información de diagnóstico detallada en el registro de Oracle ILOM para los eventos de Active Directory, establezca la propiedad Log Detail en uno de los valores de propiedad aceptados. **Sintaxis de la CLI para configuración del detalle de registro**: **set /***SP*|*CMM***/clients/activedirectory/ logdetail=***none***|***high***|***medium***|***low***|***trace*

TABLA 16 Activación de la autenticación de Active Directory *(Continuación)*

Destino configurable de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**clients/activedirectory**
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Settings (Configuración)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: se debe configurar el servidor de Active Directory con los usuarios o grupos de usuarios antes de configurar Oracle ILOM como cliente de Active Directory.**

Propiedad	Valor predeterminado	Descripción
Save (Guardar)		**Interfaz web**. Para aplicar los cambios realizados en las propiedades dentro de la página Active Directory Settings (Configuración de Active Directory), debe hacer clic en Save (Guardar).

TABLA 17 Carga o eliminación de un archivo de certificado de Active Directory

Destino configurable de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**clients/activedirectory/cert**
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Certificate Information (Información de certificado)**
- **Rol de usuario: (u) User Management (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
Certificate File Status (Estado de archivo de certificado) `(certstatus=)`	Read-Only (Sólo lectura)	*Certificate Present* |*Certificate Not Present* La propiedad Certificate File Status indica si se cargó un certificado de Active Directory en Oracle ILOM. **Precaución** – El archivo de certificado de Active Directory se debe cargar en Oracle ILOM antes de activar la propiedad Strict Certificate Mode. **Sintaxis de la CLI para mostrar certificado**: **show /***SP*|*CMM***/clients/activedirectory/cert**
File Transfer Method (Método de transferencia de archivos)	Browser (Explorador) (interfaz web únicamente)	*Browser*|*TFTP*|*FTP*|*SCP*|*Paste* Para obtener una descripción detallada de cada método de transferencia de archivos, consulte la Tabla 13.
Load Certificate (Cargar certificado) `(load_uri=)`		**Interfaz web**. Haga clic en el botón Load Certificate (Cargar certificado) para cargar el archivo de certificado de Active Directory definido en las propiedad File Transfer Method (Método de transferencia de archivos). **Sintaxis de la CLI para cargar certificado**: **load_uri=***file_transfer_method***://***host_address***/***file_path***/***filename*

TABLA 17 Carga o eliminación de un archivo de certificado de Active Directory *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/**clients/activedirectory/cert**
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Certificate Information (Información de certificado)**
- **Rol de usuario: (u) User Management (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
Remove Certificate (Eliminar certificado) (clear_action=true)		**Interfaz web**. Haga clic en el botón Remove Certificate (Eliminar certificado) para eliminar el archivo de certificado de Active Directory almacenado actualmente en Oracle ILOM. Cuando se le solicite, escriba y (Sí) para suprimirlo o n (No) para cancelar la operación. **Sintaxis de la CLI para eliminar certificado**: **set** /*SP*|*CMM*/**clients/activedirectory/cert clear_action=true** O bien: **reset** /*SP*|*CMM*/**clients/activedirectory/cert** Cuando se le solicite confirmación, escriba y para suprimirlo n para cancelar la acción.

TABLA 18 Configuración opcional de grupos de Active Directory

Destino configurable de la interfaz de usuario:
- **CLI**: /*SP*|*CMM*/`clients/activedirectory`
- **Web**: **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > (Name) Groups [(Nombre) Grupos]**
- **Rol de usuario**: **(u) User Management (requerido para todas las modificaciones de propiedades)**
- **Requisito previo**: **antes de configurar los grupos de Activity Directory en Oracle ILOM, estos grupos deben estar presentes en el servidor de Active Directory y en los miembros asignados.**

Propiedad	Descripción
Admin Groups (Grupos de administradores)	De manera opcional, un administrador del sistema puede configurar las propiedades de Admin Group en lugar de las propiedades de Role en Oracle ILOM para permitir la autorización de usuarios.
(`/admingroups/`*1*|*2*|*3*|*4*|*5*)	Oracle ILOM admite la configuración de hasta cinco grupos de administradores. Cuando se activan las propiedades de Admin Group en Oracle ILOM, se comprueba la pertenencia de un usuario a cualquiera de los grupos coincidentes definidos en la tabla de administradores. Si existe una coincidencia, se otorga al usuario acceso de nivel de administrador. **Nota**. Oracle ILOM concede al miembro de un grupo uno o más niveles de autorización en función de los grupos coincidentes (de operadores, de administradores o personalizados) detectados en la tabla de cada grupo configurado. Utilice los valores posibles siguientes para completar las propiedades de configuración para cada grupo de administradores de Active Directory en Oracle ILOM: ■ Formato de DN: CN=admingroup,OU=groups,DC=domain,DC=company,DC=com ■ Formato de dominio NT: domain\admingroup ■ Formato de dominio completo: DC=domain,DC=company,DC=com\admingroup ■ Formato de nombre simple: admingroup (Hasta 128 caracteres) **Sintaxis de la CLI para configuración de grupos de administradores:** **`set /`***SP*|*CMM***`/clients/activedirectory/admingroups/`***n*** `name=`***string* **Ejemplo de sintaxis:** **`set /SP/clients/activedirectory/admingroups/1/`** **`name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com`** `Set ?name? to ?CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com?`

TABLA 18 Configuración opcional de grupos de Active Directory *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/**clients/activedirectory**
- **Web**: **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > (Name) Groups [(Nombre) Grupos]**
- **Rol de usuario: (u) User Management (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: antes de configurar los grupos de Activity Directory en Oracle ILOM, estos grupos deben estar presentes en el servidor de Active Directory y en los miembros asignados.**

<table>
<tr><th>Propiedad</th><th>Descripción</th></tr>
<tr><td>Operator Groups (Grupos de operadores)

(/operatorgroups/1|2|3|4|5)</td><td>De manera opcional, un administrador del sistema puede configurar las propiedades de Operator Group en lugar de las propiedades de Role en Oracle ILOM para permitir la autorización de usuarios.

Oracle ILOM admite la configuración de hasta cinco grupos de operadores. Cuando se activan las propiedades de Operator Group en Oracle ILOM, se comprueba la pertenencia de un usuario a cualquiera de los grupos coincidentes definidos en la tabla de operadores. Si existe una coincidencia, se otorga al usuario acceso de nivel de operador.

Nota. Oracle ILOM concede al miembro de un grupo uno o más niveles de autorización en función de los grupos coincidentes (de operadores, de administradores o personalizados) detectados en la tabla de cada grupo configurado.

Utilice los valores posibles siguientes para completar las propiedades de configuración para cada grupo de operadores en Oracle ILOM:
■ Formato de DN: CN=operatorgroup,OU=groups,DC=domain,DC=company,DC=com
■ Formato de dominio NT: domain\operatorgroup
■ Formato de dominio completo: DC=domain,DC=company,DC=com\operatorgroup
■ Formato de nombre simple: operatorgroup
(Hasta 128 caracteres)

Sintaxis de la CLI para configuración de grupos de operadores:

set /SP|CMM/clients/activedirectory/operatorgroups/n name=string

Ejemplo de sintaxis:

set /SP/clients/activedirectory/operatorgroups/1
name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com

Set ?name? to ?CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com??</td></tr>
</table>

TABLA 18 Configuración opcional de grupos de Active Directory *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** `/`*SP*`|`*CMM*`/clients/activedirectory`
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > (Name) Groups [(Nombre) Grupos]**
- **Rol de usuario: (u) User Management (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: antes de configurar los grupos de Activity Directory en Oracle ILOM, estos grupos deben estar presentes en el servidor de Active Directory y en los miembros asignados.**

Propiedad	Descripción
Custom Groups (Grupos personalizados) (`/customgroups/`*1*`|`*2*`|`*3*`|`*4*`|`*5*)	De manera opcional, un administrador del sistema puede configurar hasta cinco propiedades de Custom Group en Oracle ILOM para permitir la autorización de usuarios. Oracle ILOM utiliza las propiedades de Custom Group para determinar los roles de usuario adecuados que se asignarán al autenticar usuarios que son miembros de un grupo personalizado. Al activar el uso de grupos personalizados en Oracle ILOM, se debe configurar tanto la propiedad Roles como la propiedad Custom Groups. Para obtener más información sobre las propiedades de configuración de los roles, consulte la propiedad Roles en la Tabla 16. **Nota**. Oracle ILOM concede al miembro de un grupo uno o más niveles de autorización en función de los grupos coincidentes (de operadores, de administradores o personalizados) detectados en la tabla de cada grupo configurado. Utilice los valores posibles siguientes para completar las propiedades de configuración para cada grupo personalizado en Oracle ILOM: ■ Rol de usuario: *administrator* |*operator*|*advanced* (a|u|c|r|o|s) ■ Formato de DN: CN=customgroup,OU=groups,DC=domain,DC=company,DC=com ■ Formato de dominio NT: domain\customgroup ■ Formato de dominio completo: DC=domain,DC=company,DC=com\customgroup ■ Formato de nombre simple: customgroup (Hasta 128 caracteres) **Sintaxis de la CLI para configuración de grupos personalizados:** **`set /`***SP*|*CMM***`/clients/activedirectory/customgroups/`***n*** `name=`***string* **`roles=`***administrator*|*operator*|*a*|*u*|*c*|*r*|*o*|*s* **Ejemplo de sintaxis:** **`set /SP/clients/activedirectory/customgroups/1`** **`name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com roles=au`** Set ?name? to ?CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com?? roles? to ?au? **Información relacionada**: ■ “Roles de usuario asignables de Oracle ILOM” en la página 40
Save (Guardar)	**Interfaz web**. Para aplicar los cambios realizados en las propiedades de los cuadros de diálogo Admin, Operator o Custom Group (Grupo de administradores, de operadores o personalizado), debe hacer clic en Save (Guardar).

TABLA 19 Configuración de dominios de usuario de Active Directory

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/activedirectory/userdomains/***n*
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > User Domains (Dominios de usuario)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: antes de configurar los dominios de usuario de Activity Directory en Oracle ILOM, estos dominios deben estar presentes en el servidor de Active Directory y en los miembros asignados.**

Propiedad	Descripción
User Domains (Dominios de usuario) (*1*|*2*|*3*|*4*|*5*)	De manera opcional, un administrador del sistema puede configurar hasta cinco dominios de usuario. Cuando se definen uno o varios dominios de usuario, Oracle ILOM utiliza estas propiedades en orden consecutivo hasta que puede autenticar el usuario de Active Directory. Utilice los valores posibles siguientes para completar las propiedades de configuración para cada dominio de usuario en Oracle ILOM: ■ Formato de UPN: <USERNAME>@domain.company.com ■ Formato de DN: CN=<USERNAME>,CN=Users,DC=domain,DC=company,DC=com **Nota –** Puede utilizar <USERNAME> como valor literal. Cuando se utiliza <USERNAME> como valor literal, Oracle ILOM reemplaza <USERNAME> por el nombre de inicio de sesión actual durante la autenticación de usuarios. **Sintaxis de la CLI para dominios de usuario:** **set /***SP*|*CMM***/clients/activedirectory/userdomains/***n* **name=***string* **Ejemplo 1:** `name=CN=<USERNAME>` **set /SP/clients/activedirectory/userdomains/1/name=CN<USERNAME>, OU=Groups, DC=sales, DC-Oracle, DC=com** Set ?name? to ?CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com? **Ejemplo 2:** name=CN=spSuperAdmin **set /SP/clients/activedirectory/userdomains/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com** `Set ?name? to ?CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com?`
Save (Guardar)	**Interfaz web**. Para aplicar los cambios realizados en las propiedades del cuadro de diálogo Active Directory User Domains (Dominios de usuario de Active Directory), debe hacer clic en Save (Guardar).

TABLA 20 Configuración opcional de servidores alternativos de Active Directory

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/clients/activedirectory/alternateservers/*n*
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > Alternate Servers (Servidores alternativos)
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)

Propiedad	Descripción
Alternate Servers (Servidores alternativos) (/*1*|*2*|*3*|*4*|*5*)	Oracle ILOM permite que un administrador del sistema configure hasta cinco servidores alternativos de Active Directory. Los servidores alternativos ofrecen redundancia de autenticación, además de una selección de diferentes servidores de Active Directory para utilizar cuando sea necesario aislar dominios. Cada servidor alternativo de Active Directory utiliza los mismos requisitos y reglas de autorización de usuarios que el servidor de Active Directory principal. Por ejemplo, Oracle ILOM utilizará los roles de usuario configurados en la propiedad Roles para autenticar usuarios. Sin embargo, si no se configura la propiedad Roles, Oracle ILOM consultará el servidor de autenticación para comprobar los roles de autorización adecuados. Cada servidor alternativo de Active Directory tiene sus propias propiedades para dirección de red, puerto, estado de certificado y comandos para cargar y eliminar certificados. Si no se proporciona ningún certificado de Active Directory, pero se necesita uno, Oracle ILOM utilizará el certificado de nivel superior del servidor de Active Directory principal. **Nota** – Si los servidores alternativos se utilizan para proporcionar redundancia de autenticación, se puede activar la propiedad para Strict Credential Error Mode (Modo de error de credenciales estricto). No obstante, si los servidores alternativos abarcan dominios no contiguos, se deberá desactivar la propiedad para Strict Credential Error Mode. Para conocer las propiedades de configuración de Strict Credential Error Mode, consulte la Tabla 16. **Sintaxis de la CLI para dirección y puerto de servidores alternativos:** **set /***SP*|*CMM***/clients/activedirectory/alternateservers/***n* **address=***string* **port=***string* **Sintaxis de la CLI para certificado de servidores alternativos:** **show /***SP*|*CMM***/clients/activedirectory/alternateservers/***n***/cert** **load_uri=***file_transfer_method***://***host_address***/***file_path***/***filename* **set /***SP*|*CMM***/clients/activedirectory/alternateservers/***n***/cert clear_action=true**
Save (Guardar)	**Interfaz web**. Para aplicar los cambios realizados en las propiedades del cuadro de diálogo Active Directory Alternate Servers (Servidores alternativos de Active Directory), debe hacer clic en Save (Guardar).

TABLA 21 Edición opcional de consultas del localizador de DNS

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/activedirectory/dnslocatorqueries**
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > Active Directory > DNS Locator Queries (Consultas del localizador de DNS)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
DNS Locator Queries (Consultas del localizador de DNS) (/1)	_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>	Oracle ILOM permite configurar hasta cinco consultas del localizador de DNS. Una consulta del localizador de DNS identifica el servicio DNS con nombre y el ID de puerto. El ID de puerto suele formar parte del registro, pero se puede anular con el formato <PORT:636>. Además, puede anular el servicio DNS con nombre de un dominio específico con el marcador de sustitución <DOMAIN>. **Sintaxis de la CLI para mostrar y editar consultas del localizador de DNS:** **show** /*SP*|*CMM*/**clients/activedirectory/dnslocatorqueries/1** **set** /*SP*|*CMM*/clients/activedirectory/dnslocatorqueries/1 service = *string* **Ejemplo de sintaxis de consultas del localizador de DNS para** `service= string` service =_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:*nnnn*>
DNS Locator Queries (Consultas del localizador de DNS) (/2)	_ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>	
Save (Guardar)		**Interfaz web**. Para aplicar los cambios realizados en las propiedades del cuadro de diálogo Active Directory DNS Locator Queries (Consultas del localizador de DNS de Active Directory), debe hacer clic en Save (Guardar).

TABLA 22 Directrices para resolver problemas con la autenticación de Active Directory

Consulte las siguientes directrices al resolver problemas relacionados con los intentos de autenticación y autorización de Active Directory en Oracle ILOM.

- Para probar y diagnosticar la autenticación de Active Directory, siga estos pasos:
  1. Establezca la propiedad Log Detail (Detalle de registro) de Active Directory en `trace`.
  2. Intente realizar una autenticación en Oracle ILOM para generar eventos.
  3. Consulte el archivo de registro de eventos de Oracle ILOM.
- Asegúrese de que los grupos de usuarios y dominios de usuario configurados en el servidor de Active Directory coincidan con los grupos de usuarios y dominios de usuario configurados en Oracle ILOM.
- El cliente de Active Directory de Oracle ILOM no gestiona la configuración del reloj. La configuración del reloj en Oracle ILOM se define manualmente o a través de un servidor NTP.
  Nota. Cuando la configuración del reloj en Oracle ILOM se define con un servidor NTP, Oracle ILOM realiza una operación ntpdate con el servidor NTP antes de iniciar el daemon NTP.

TABLA 22 Directrices para resolver problemas con la autenticación de Active Directory *(Continuación)*

Información relacionada:

- Tabla 16
- *User?s Guide*, Managing Oracle ILOM Log Entries
- "Configuración de propiedades para el reloj del SP o el CMM " en la página 123

Configuración de LDAP/SSL

De manera opcional, los administradores del sistema pueden configurar Oracle ILOM para utilizar el servicio de directorio LDAP/SSL a fin de autenticar los usuarios de Oracle ILOM, así como definir los niveles de autorización de usuarios para las funciones dentro de Oracle ILOM.

La propiedad para el estado del servicio LDAP/SSL está desactivada de forma predeterminada en Oracle ILOM. Para activar el estado del servicio LDAP/SSL y configurar Oracle ILOM como cliente LDAP/SSL, consulte las siguientes tablas:

- Tabla 23
- Tabla 24
- Tabla 25
- Tabla 26
- Tabla 27
- Tabla 28

TABLA 23 Activación de la autenticación LDAP/SSL

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/ldapssl/**
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Settings (Configuración)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo:** **se debe configurar el servidor LDAP/SSL con los usuarios o grupos de usuarios antes de configurar Oracle ILOM.**

Propiedad	Valor predeterminado	Descripción
State (Estado) (`state=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Para configurar Oracle ILOM para utilizar el servicio de directorio de autenticación y autorización LDAP/SSL, establezca el estado de la propiedad State en activado. Cuando se desactiva la propiedad State, Oracle ILOM no puede utilizar el servicio LDAP/SSL para los niveles de autenticación y autorización de usuarios. Cuando se activa la propiedad State y se desactiva la propiedad Strict Certificate Mode (Modo de certificado estricto), Oracle ILOM proporciona a través de un canal seguro una validación limitada del certificado del servicio LDAP/SSL durante la autenticación de usuarios. Cuando se activa la propiedad State y también se activa la propiedad Strict Certificate Mode, Oracle ILOM realiza a través de un canal seguro una verificación completa de las firmas digitales del certificado del servicio LDAP/SSL durante la autenticación de usuarios. **Sintaxis de la CLI para estado**: **set /***SP*|*CMM***/clients/ldapssl/ state=***disabled*|*enabled*

TABLA 23 Activación de la autenticación LDAP/SSL *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** `/`*SP*`|`*CMM*`/clients/ldapssl/`
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Settings (Configuración)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo:** **se debe configurar el servidor LDAP/SSL con los usuarios o grupos de usuarios antes de configurar Oracle ILOM.**

Propiedad	Valor predeterminado	Descripción
Roles (`defaultrole=`)	None (server authorization) [Ninguno (autorización de servidor)]	*Administrator* |*Operator* |*Advanced* |*None* (server authorization) Para definir qué funciones de Oracle ILOM estarán disponibles para los usuarios autenticados de LDAP/SSL, establezca la propiedad Roles predeterminada en uno de los cuatro valores de propiedad aceptados: Administrator (a|u|c|r|o), Operator (c|r|o), Advanced (*a*|*u*|*c*|*r*|*o*|*s*) o None (server authorization). Cuando se establece la propiedad Roles predeterminada en un rol de usuario de Oracle ILOM, los niveles de autorización para usar las funciones dentro de Oracle ILOM estarán determinados por los privilegios de usuario otorgados mediante el rol de usuario de Oracle ILOM. Para obtener una descripción de los privilegios asignados, consulte las tablas que se enumeran a continuación en la sección Información relacionada para conocer los roles y los perfiles de usuario. Cuando se establece la propiedad Roles predeterminada en `None (server authorization)` y se configura Oracle ILOM para utilizar los grupos LDAP/SSL, los niveles de autorización para usar las funciones dentro de Oracle ILOM estarán determinados por el grupo LDAP/SSL. Para obtener detalles adicionales sobre la configuración de LDAP/SSL, consulte la tabla que describe los grupos LDAP/SSL que se enumeran a continuación en la sección Información relacionada. **Sintaxis de la CLI para roles**: **`set /`***SP*|*CMM***`/clients/ldapssl/`** **`defaultrole=`***administrator***|***operator***|***a***|***u***|***c***|***r***|***o***|***s***|***none* **Información relacionada:** ■ Tabla 9 ■ Tabla 10 ■ Tabla 25

TABLA 23 Activación de la autenticación LDAP/SSL *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/ldapssl/**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Settings (Configuración)
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)
- **Requisito previo:** se debe configurar el servidor LDAP/SSL con los usuarios o grupos de usuarios antes de configurar Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
Address (Dirección) `(address=)`	0.0.0.0	*IP address*| *DNS host name* (servidor de Active Directory) Para configurar la dirección de red del servidor LDAP/SSL, complete la propiedad Address con la dirección IP de LDAP/SSL o el nombre de host DNS. Si se utiliza un nombre de host DNS, las propiedades de configuración de DNS deberán estar definidas y activadas correctamente en Oracle ILOM. **Sintaxis de la CLI para dirección**: **set /***SP*|*CMM***/clients/ldapssl/ address=***LDAP/SSL_server ip_address***|***active_directory_server_dns_host_name* **Información relacionada:** ■ Tabla 44
Port (Puerto) `(port=)`	0 Auto-select (Selección automática)	*0 Auto-select* | *Non-standard TCP port* Oracle ILOM utiliza un puerto TCP estándar para comunicarse con el servidor LDAP/SSL. Cuando se activa la propiedad Port: Auto-select, el número de puerto se establece en 0 de forma predeterminada. Cuando se desactiva la propiedad Port: Auto-select, el usuario puede configurar la propiedad de número de puerto de la interfaz web. Se proporciona una propiedad Port configurable en el caso poco probable de que Oracle ILOM necesite usar un puerto TCP no estándar. **Sintaxis de la CLI para puerto**: **set /***SP*|*CMM***/clients/ldapssl/ port=***number*
Timeout (Tiempo de espera) `(timeout=)`	4 segundos	*4* |*user-specified* La propiedad Timeout se establece en 4 segundos de forma predeterminada. Si es necesario, ajuste el valor de esta propiedad para optimizar el tiempo de respuesta para los casos en que el servidor LDAP/SSL no esté disponible o no responda. La propiedad Timeout designa la cantidad de segundos que se debe esperar para que se complete una transacción individual. El valor no representa el tiempo total que tardan en completarse todas las transacciones, ya que la cantidad de transacciones puede variar según la configuración. **Sintaxis de la CLI para tiempo de espera**: **set /***SP*|*CMM***/clients/ldapssl/ timeout=***number_of_seconds*

TABLA 23 Activación de la autenticación LDAP/SSL *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** `/`*SP*`|`*CMM*`/clients/ldapssl/`
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Settings (Configuración)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: se debe configurar el servidor LDAP/SSL con los usuarios o grupos de usuarios antes de configurar Oracle ILOM.**

Propiedad	Valor predeterminado	Descripción
Strict Certificate Mode (Modo de certificado estricto) (`strictcert mode=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Cuando se activa, Oracle ILOM realiza una verificación completa de las firmas del certificado de LDAP/SSL durante la autenticación a través de un canal seguro. Cuando se desactiva, Oracle ILOM proporciona una validación limitada del certificado del servidor durante la autenticación a través de un canal seguro. **Precaución –** El certificado del servidor LDAP/SSL se debe cargar en Oracle ILOM antes de activar la propiedad Strict Certificate Mode. **Sintaxis de la CLI para modo de certificado estricto**: **`set /`***SP*|*CMM***`/clients/ldapssl/ strictcertmode=`***disabled*|*enabled* **Información relacionada**: ■ Tabla 24

TABLA 23 Activación de la autenticación LDAP/SSL *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/**clients/ldapssl/**
- **Web**: **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Settings (Configuración)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: se debe configurar el servidor LDAP/SSL con los usuarios o grupos de usuarios antes de configurar Oracle ILOM.**

Propiedad	Valor predeterminado	Descripción
Optional User Mapping (Asignación opcional de usuarios) (`/optionalUsermapping`)	Disabled (Desactivado)	*Disabled* | *Enabled* Por lo general, la propiedad Optional User Mapping se utiliza cuando no se usó un `uid` como parte del nombre de inicio de sesión del dominio de usuario. Establezca el estado de la propiedad Optional User Mapping en activado si es necesario convertir nombres de inicio de sesión de usuario simples en nombres de dominio para la autenticación de usuarios. ■ State (Estado): cuando se activa, es posible configurar atributos alternativos para la autenticación de credenciales de usuario. ■ Attribute Information (Información de atributo): especifique la información de inicio de sesión del atributo con el formato de entrada aceptado (&(objectclass=person)(uid=<USERNAME>)). La información del atributo permite que la consulta LDAP/SSL busque nombres de dominio de usuario en función de la información de inicio de sesión del atributo que se proporcionó. ■ Searchbase (Base de búsqueda): establezca la propiedad Searchbase en el nombre distintivo del objeto de base de búsqueda o en una rama del árbol LDAP en el que Oracle ILOM debe buscar las cuentas de usuario LDAP. Formato de entrada: `OU={organization},DC={company},DC={com}` ■ Bind DN (DN de enlace): establezca la propiedad Bind DN en el nombre distintivo (DN) de un usuario proxy con acceso de sólo lectura en el servidor LDAP. Oracle ILOM debe tener acceso de sólo lectura en el servidor LDAP para buscar y autenticar usuarios. Formato de entrada: `OU={organization},DC={company},DC={com}` ■ Bind Password (Contraseña de enlace): establezca la propiedad Bind Password en una contraseña para el usuario proxy con acceso de sólo lectura. **Sintaxis de la CLI para asignación opcional de usuarios**: **set /***SP*|*CMM***/clients/ldapssl/optionalUsermapping/ attributeInfo=<string> searchbase=<string> binddn=cn=***proxyuser*, **ou=***organization _name*, **dc=***company*, **dc=com bindpw=***password*

TABLA 23 Activación de la autenticación LDAP/SSL *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** `/`*SP*`|`*CMM*`/clients/ldapssl/`
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Settings (Configuración)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo:** **se debe configurar el servidor LDAP/SSL con los usuarios o grupos de usuarios antes de configurar Oracle ILOM.**

Propiedad	Valor predeterminado	Descripción
Log Detail (Detalle de registro) (`logdetail=`)	None (Ninguno)	*None* | *High* | *Medium* | *Low* |*Trace* Para especificar el tipo de información de diagnóstico detallada en el registro de Oracle ILOM para los eventos de LDAP/SSL, establezca la propiedad Log Detail en uno de los cinco valores de propiedad aceptados (ninguno, alto, medio, bajo o seguimiento). **Sintaxis de la CLI para detalle de registro**: **`set /`***SP*|*CMM***`/clients/ldapssl/ logdetail=`***none***`|`***high***`|`***medium***`|`***low***`|`***trace*
Save (Guardar)		**Interfaz web**. Para aplicar los cambios realizados en las propiedades dentro de la página LDAP/SSL Settings (Configuración de LDAP/SSL), debe hacer clic en Save (Guardar).

TABLA 24 Carga o eliminación de un archivo de certificado de LDAP/SSL

Destino configurable de la interfaz de usuario:

- **CLI:** `/`*SP*`|`*CMM*`/clients/ldapssl/cert`
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Certificate Information (Información de certificado)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
Certificate File Status (Estado de archivo de certificado) (`certstatus=`)	Read-Only (Sólo lectura)	*Certificate Present* |*Certificate Not Present* La propiedad Certificate File Status indica si se cargó un certificado de LDAP/SSL en Oracle ILOM. **Sintaxis de la CLI para estado de certificado**: **`show /`***SP*|*CMM***`/clients/ldapssl/cert`**
File Transfer Method (Método de transferencia de archivos)	Browser (Explorador) (interfaz web únicamente)	*Browser*|*TFTP*|*FTP*|*SCP*|*Paste* Para obtener una descripción detallada de cada método de transferencia de archivos, consulte la Tabla 13.
Load Certificate (Cargar certificado) (`load_uri=`)		**Interfaz web.** Haga clic en el botón Load Certificate (Cargar certificado) para cargar el archivo de certificado de LDAP/SSL designado en la propiedad File Transfer Method (Método de transferencia de archivos). **Sintaxis de la CLI para cargar certificado**: **`load_uri=`***file_transfer_method***`://`***host_address***`/`***file_path***`/`***filename*

TABLA 24 Carga o eliminación de un archivo de certificado de LDAP/SSL *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/ldapssl/cert**
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Certificate Information (Información de certificado)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
Remove Certificate (Eliminar certificado) (`clear_action=true`)		**Interfaz web**. Haga clic en el botón Remove Certificate (Eliminar certificado) para eliminar el archivo de certificado de LDAP/SSL almacenado actualmente en Oracle ILOM. Cuando se le solicite, haga clic en Yes (Sí) para continuar con la acción o en No para cancelarla. **Sintaxis de la CLI para eliminar certificado**: **set** /*SP*|*CMM*/**clients/ldapssl/cert clear_action=true** O bien: **reset** /*SP*|*CMM*/**clients/ldapssl/cert** Cuando se le solicite, escriba `y` para continuar con la acción o `n` para cancelarla.

TABLA 25 Configuración opcional de grupos LDAP/SSL

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/ldapssl**
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > (Name) Groups [(Nombre) Grupos]**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: antes de configurar los grupos LDAP/SSL en Oracle ILOM, estos grupos deben estar presentes en el servidor LDAP/SSL y en los miembros asignados.**

Propiedad	Descripción
Admin Groups (Grupos de administradores) (/admingroups/*1*|*2*|*3*|*4*|*5*)	De manera opcional, un administrador del sistema puede configurar las propiedades de Admin Group en lugar de las propiedades de Role en Oracle ILOM para permitir la autorización de usuarios. Oracle ILOM admite la configuración de hasta cinco grupos de administradores. Cuando se activan las propiedades de Admin Group en Oracle ILOM, se comprueba la pertenencia de un usuario a cualquiera de los grupos coincidentes definidos en la tabla de administradores. Si existe una coincidencia, se otorga al usuario acceso de nivel de administrador. **Nota**. Oracle ILOM concede al miembro de un grupo uno o más niveles de autorización en función de los grupos coincidentes (de operadores, de administradores o personalizados) detectados en la tabla de cada grupo configurado. **Sintaxis de la CLI para grupo de administradores:** **set /***SP*|*CMM***/clients/ldapssl/admingroups/***n* **name=***string* **Ejemplo de sintaxis:** **set /SP/clients/ldapssl/admingroups/1/** **name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com** Set ?name? to ?CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com?
Operator Groups (Grupos de operadores) (/operatorgroups/*1*|*2*|*3*|*4*|*5*)	De manera opcional, un administrador del sistema puede configurar las propiedades de Operator Group en lugar de las propiedades de Role en Oracle ILOM para permitir la autorización de usuarios. Oracle ILOM admite la configuración de hasta cinco grupos de operadores. Cuando se activan las propiedades de Operator Group en Oracle ILOM, se comprueba la pertenencia de un usuario a cualquiera de los grupos coincidentes definidos en la tabla de operadores. Si existe una coincidencia, se otorga al usuario acceso de nivel de operador. **Nota**. Oracle ILOM concede al miembro de un grupo uno o más niveles de autorización en función de los grupos coincidentes (de operadores, de administradores o personalizados) detectados en la tabla de cada grupo configurado. **Sintaxis de la CLI para grupo de operadores:** **set /***SP*|*CMM***/clients/ldapssl/operatorgroups/***n* **name=***string* **Ejemplo de sintaxis:** **set /SP/clients/ldapssl/operatorgroups/1** **name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com** Set ?name? to ?CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com??

TABLA 25 Configuración opcional de grupos LDAP/SSL *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/ldapssl**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > (Name) Groups [(Nombre) Grupos]
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)
- **Requisito previo:** antes de configurar los grupos LDAP/SSL en Oracle ILOM, estos grupos deben estar presentes en el servidor LDAP/SSL y en los miembros asignados.

Propiedad	Descripción
Custom Groups (Grupos personalizados) (/customgroups/*1*|*2*|*3*|*4*|*5*)	De manera opcional, un administrador del sistema puede configurar hasta cinco propiedades de Custom Groups en Oracle ILOM para permitir la autorización de usuarios. Oracle ILOM utiliza las propiedades de Custom Group para determinar los roles de usuario adecuados que se asignarán al autenticar usuarios que son miembros de un grupo personalizado. Al activar el uso de grupos personalizados en Oracle ILOM, se debe configurar tanto la propiedad Roles como la propiedad Custom Groups. Para obtener más información sobre las propiedades de configuración de los roles, consulte la propiedad Roles en la Tabla 23. **Nota**. Oracle ILOM concede al miembro de un grupo uno o más niveles de autorización en función de los grupos coincidentes (de operadores, de administradores o personalizados) detectados en la tabla de cada grupo configurado. **Sintaxis de la CLI para grupos personalizados:** **set** /*SP*|*CMM*/**clients/ldapssl/customgroups/***n* **name=***string* **roles=***administrator*|*operator*|*a*|*u*|*c*|*r*|*o*|*s* **Ejemplo de sintaxis:** **set /SP/clients/ldapssl/customgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com roles=au** `Set ?name? to ?CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com?? roles? to ?au?` **Información relacionada**: ■ "Roles de usuario asignables de Oracle ILOM" en la página 40
Save (Guardar)	**Interfaz web**. Para aplicar los cambios realizados en las propiedades de los cuadros de diálogo Admin, Operator o Custom Group (Grupo de administradores, de operadores o personalizado), debe hacer clic en Save (Guardar).

TABLA 26 Configuración de dominios de usuario de LDAP/SSL

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/ldapssl/userdomains/***n*
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > User Domains (Dominios de usuario)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito previo: antes de configurar los dominios de usuario en Oracle ILOM, estos dominios deben estar presentes en el servidor LDAP/SSL y en los miembros asignados.**

<table>
<tr><th>Propiedad</th><th>Descripción</th></tr>
<tr><td>User Domains (Dominios de usuario)

(/<i>1</i>|<i>2</i>|<i>3</i>|<i>4</i>|<i>5</i></td><td>De manera opcional, un administrador del sistema puede configurar hasta cinco dominios de usuario. Cuando se definen uno o varios dominios de usuario, Oracle ILOM utiliza estas propiedades en orden consecutivo hasta que puede autenticar el usuario de LDAP/SSL.

Utilice los valores posibles siguientes para completar las propiedades de configuración para cada dominio de usuario en Oracle ILOM.
Formato de UID: uid=<USERNAME>,ou=people,dc=company,dc=com
Formato de DN: CN=<USERNAME>,CN=Users,DC=domain,DC=company,DC=com
Nota – Puede utilizar <USERNAME> como valor literal. Cuando se utiliza <USERNAME> como valor literal, Oracle ILOM reemplaza <USERNAME> por el nombre de inicio de sesión actual durante la autenticación de usuarios.

Puede especificar una base de búsqueda de manera opcional. Para ello, anexe la propiedad <BASE:<i>string</i>> después de la configuración del dominio de usuario. Para obtener detalles de la sintaxis, consulte el ejemplo 3 a continuación.

Sintaxis de la CLI para dominios de usuario:

set /<i>SP</i>|<i>CMM</i>/clients/ldapssl/userdomains/<i>n</i> domain=<i>string</i>

Ejemplo 1: domain=CN=<USERNAME>

set /SP/clients/ldapssl/userdomains/1
domain=CN=<USERNAME>,OU=Groups,DC=sales,DC-oracle,DC=com

Set ?domain? to ?CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com?

Ejemplo 2: domain=CN=spSuperAdmin

set /SP/clients/ldapssl/userdomains/1
domain=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com

Set ?domain? to ?CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com?

Ejemplo 3: Sintaxis de la base de búsqueda con <BASE:<i>string</i>>

set /SP/clients/ldapssl/userdomains/1
domain=uid=<USERNAME>,ou=people,dc=oracle,dc=com<BASE:ou=doc,dc=oracle,dc=com></td></tr>
<tr><td>Save (Guardar)</td><td>Interfaz web. Para aplicar los cambios realizados en las propiedades del cuadro de diálogo LDAP/SSL User Domain (Dominio de usuario de LDAP/SSL), debe hacer clic en Save (Guardar).</td></tr>
</table>

TABLA 27 Configuración opcional de servidores alternativos LDAP/SSL

Destino configurable de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/**clients/ldapssl/alternateservers/***n*
- **Web: ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP/SSL > Alternate Servers (Servidores alternativos)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**

Propiedad	Descripción
Alternate Servers (Servidores alternativos) (/*1*|*2*|*3*|*4*|*5*)	Oracle ILOM permite configurar hasta cinco servidores alternativos LDAP/SSL. Los servidores alternativos ofrecen redundancia de autenticación, además de una selección de diferentes servidores LDAP/SSL para utilizar cuando sea necesario aislar dominios. Cada servidor alternativo LDAP/SSL utiliza los mismos requisitos y reglas de autorización de usuarios que el servidor LDAP/SSL principal. Por ejemplo, Oracle ILOM utilizará los roles de usuario configurados en la propiedad Roles para autenticar usuarios. Sin embargo, si no se configura la propiedad Roles, Oracle ILOM consultará el servidor de autenticación para comprobar los roles de autorización adecuados. Cada servidor alternativo tiene sus propias propiedades para dirección de red, puerto, estado de certificado y comandos para cargar y eliminar certificados. Si no se proporciona ningún certificado de LDAP/SSL, pero se necesita uno, Oracle ILOM utilizará el certificado de nivel superior del servidor LDAP/SSL principal. **Sintaxis de la CLI para dirección y puerto de servidores alternativos:** **set /***SP*|*CMM***/clients/ldapssl/alternateservers/***n* **address=***string* **port=***string* **Sintaxis de la CLI para certificado de servidores alternativos:** **show /***SP*|*CMM*/**clients/ldapssl/alternateservers/***n***/cert** **load_uri=***file_transfer_method***://***host_address***/***file_path***/***filename* **set /***SP*|*CMM***/clients/ldapssl/alternateservers/***n***/cert clear_action=true**
Save (Guardar)	**Interfaz web**. Para aplicar los cambios realizados en las propiedades del cuadro de diálogo LDAP/SSL Alternate Servers (Servidores alternativos LDAP/SSL), debe hacer clic en Save (Guardar).

TABLA 28 Directrices para resolver problemas con la autenticación LDAP/SSL

Consulte las siguientes directrices al resolver problemas relacionados con los intentos de autenticación y autorización LDAP/SSL en Oracle ILOM.

- Para probar la autenticación LDAP/SSL y configurar el registro de Oracle ILOM para que realice un seguimiento de los eventos de LDAP/SSL, siga estos pasos:

  1. Establezca la propiedad Log Detail (Detalle de registro) de LDAP/SSL en trace.

  2. Intente realizar una autenticación en Oracle ILOM para generar eventos.

  3. Consulte el archivo de registro de eventos de Oracle ILOM.
- Asegúrese de que los grupos de usuarios y dominios de usuario configurados en el servidor LDAP/SSL coincidan con los grupos de usuarios y dominios de usuario configurados en Oracle ILOM.
- El cliente LDAP/SSL de Oracle ILOM no gestiona la configuración del reloj. La configuración del reloj en Oracle ILOM se define manualmente o a través de un servidor NTP.

  Nota. Cuando la configuración del reloj en Oracle ILOM se define con un servidor NTP, Oracle ILOM realiza una operación ntpdate con el servidor NTP antes de iniciar el daemon NTP.

Información relacionada:

- Tabla 23
- *User?s Guide*, Managing Oracle ILOM Log Entries
- "Configuración de propiedades para el reloj del SP o el CMM " en la página 123

Configuración de LDAP

Los administradores del sistema pueden configurar Oracle ILOM a fin de usar el servicio del protocolo ligero de acceso a directorios (LDAP) para autenticar los usuarios. Este servicio está basado en un modelo de consulta de cliente/servidor que utiliza una cuenta de usuario proxy con acceso de sólo lectura a fin de consultar el servidor LDAP para la autenticación de usuarios.

La propiedad para el estado del servicio LDAP está desactivada de forma predeterminada en Oracle ILOM. Para activar el estado del servicio LDAP y configurar propiedades a fin de usar el servicio de directorio LDAP para la autenticación de usuarios, consulte estas tablas:

- Tabla 29
- Tabla 30

TABLA 29 Requisitos para activar Oracle ILOM como cliente LDAP

Antes de configurar Oracle ILOM como cliente LDAP, se debe configurar correctamente el servidor LDAP. Consulte las siguientes directrices y la sección Información relacionada al configurar el servidor LDAP para que reconozca Oracle ILOM como cliente LDAP.

- Asegúrese de que el servidor LDAP esté configurado para usar el formato {crypt} de la contraseña predeterminada. Las contraseñas de todos los usuarios de LDAP que se autentican en Oracle ILOM deben almacenarse en uno de los dos formatos {crypt} siguientes:

  `userPassword: {CRYPT}ajCa2He4PJhNo`

  `userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46`

- Consulte el esquema de Internet Engineering Task Force (RFC 2307) para agregar clases de objeto para `posixAccount` y `shadowAccount` y luego completar los valores de propiedad necesarios para:
  - *uidnumber*
  - *gidnumber*
  - *uid* (nombre de usuario de Oracle ILOM)
- Permita que el servidor LDAP acepte enlaces anónimos o cree un usuario proxy en el servidor LDAP que tenga acceso de sólo lectura para todas las cuentas de usuario que se autentiquen en Oracle ILOM.

Información relacionada:

- Esquema de Internet Engineering Task Force (RC2307) (`http://www.ietf.org/rfc/rfc2307.txt`)

TABLA 30 Configuración de Oracle ILOM para usar la autenticación LDAP

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/ldap**
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP Settings (Configuración de LDAP)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
State (Estado) (`state=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Para permitir que Oracle ILOM autentique usuarios con el servicio de directorio LDAP, establezca el estado de la propiedad State en activado. Cuando se activa la propiedad State, Oracle ILOM consulta el servidor LDAP para autenticar los usuarios de LDAP. **Sintaxis de la CLI para estado**: **set /***SP*|*CMM***/clients/ldap/ state=***disabled*|*enabled*

TABLA 30 Configuración de Oracle ILOM para usar la autenticación LDAP *(Continuación)*

Destino configurable de la interfaz de usuario:
- **CLI:** `/`*SP*`|`*CMM*`/clients/ldap`
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP Settings (Configuración de LDAP)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
Roles (`defaultrole=`)	Operator (Operador)	*Administrator* |*Operator* |*Advanced* Para definir qué funciones de Oracle ILOM estarán disponibles para los usuarios autenticados de LDAP, establezca la propiedad Roles predeterminada en uno de los tres roles de usuario de Oracle ILOM: Administrator (a|u|c|r|o), Operator (c|r|o) o Advanced (*a*|*u*|*c*|*r*|*o*|*s*). Los niveles de autorización para usar funciones dentro de Oracle ILOM están determinados por los privilegios de usuario otorgados por el rol de usuario configurado de Oracle ILOM. Para obtener una descripción de los privilegios asignados, consulte los temas sobre roles de usuario y perfiles de usuario que se enumeran a continuación en la sección Información relacionada. **Sintaxis de la CLI para roles**: **set /***SP*|*CMM***/clients/ldap/ defaultrole=***administrator*|*operator*|*a*|*u*|*c*|*r*|*o*|*s* **Información relacionada:** ▪ Tabla 9 ▪ Tabla 10
Address (Dirección) (`address=`)	0.0.0.0	*IP address*| *DNS host name* (servidor LDAP) Para configurar la dirección de red del servidor LDAP, complete la propiedad Address con la dirección IP del servidor LDAP o el nombre de host DNS. Si se utiliza un nombre de host DNS, las propiedades de configuración de DNS deberán estar definidas y activadas correctamente en Oracle ILOM. **Sintaxis de la CLI para dirección**: **set /***SP*|*CMM***/clients/ldap/ address=***ldap_server ip_address*|*ldap_server_dns_host_name* **Información relacionada:** ▪ Tabla 44
Port (Puerto) (`port=`)	389	*389* | *User-specified TCP port* Oracle ILOM utiliza el puerto TCP 389 para comunicarse con el servidor OpenLDAP. Si es necesario, configure Oracle ILOM para que utilice otro puerto. Para ello, modifique el número de puerto predeterminado: 389 **Sintaxis de la CLI para puerto**: **set /***SP*|*CMM***/clients/ldap/ port=***number*

TABLA 30 Configuración de Oracle ILOM para usar la autenticación LDAP *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/ldap**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > LDAP Settings (Configuración de LDAP)
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)

Propiedad	Valor predeterminado	Descripción
Searchbase (Base de búsqueda) (searchbase=)		ou=*organization_unit* |dn=*domain_name*|dc=*domain*| La base de búsqueda representa la ubicación en el árbol LDAP donde ILOM realiza búsquedas para validar las credenciales de usuario. Utilice el formato de entrada aceptado para completar la propiedad Searchbase con un nombre distintivo para el objeto de base de búsqueda o con la rama del árbol LDAP en el que Oracle ILOM debe buscar las cuentas de usuario LDAP. Por ejemplo, para buscar en el contenedor IT del dominio MyCompany.com, deberá especificar esta base de búsqueda: ou=IT, dc=mycompany, dc=.com **Sintaxis de la CLI para base de búsqueda**: **set /***SP*|*CMM***/clients/ldap/ searchbase= ou=***organization_name***,** **dn=***domain_name*, **dc**=*domain*
Bind DN (DN de enlace) (binddn=)		ou=*organization_unit* |dn=*domain_name*|dc=*domain*|cn=*common_name* Para otorgar a Oracle ILOM acceso de sólo lectura en el servidor LDAP, complete la propiedad Bind DN con un nombre distintivo (DN) para un usuario proxy con acceso de sólo lectura. **Nota**. Oracle ILOM debe tener acceso de sólo lectura en el servidor LDAP para buscar y autenticar usuarios de LDAP. **Sintaxis de la CLI para DN de enlace**: **set /***SP*|*CMM***/clients/ldap/ binddn=cn=***proxyuser***, ou=***organization _name,* **dc=***domain*
Bind Password (Contraseña de enlace) (bindpw=)		Para proporcionar en Oracle ILOM una contraseña para el usuario proxy con acceso de sólo lectura, complete la propiedad Bind Password con una contraseña. **Sintaxis de la CLI para contraseña de enlace**: **set /***SP*|*CMM***/clients/ldap/ bindpw=***password*
Save (Guardar)		**Interfaz web**. Para aplicar los cambios realizados en las propiedades dentro de la página LDAP Settings (Configuración de LDAP), debe hacer clic en Save (Guardar).

Configuración de RADIUS

Los administradores del sistema pueden configurar Oracle ILOM a fin de usar un servicio de autenticación remota telefónica de usuario (RADIUS) para autenticar los usuarios. Este servicio está basado en un modelo de consulta de cliente/servidor que utiliza una contraseña de tipo secreto compartido para autenticar los usuarios. El cliente RADIUS y el servidor RADIUS de Oracle ILOM deben conocer la contraseña de tipo secreto compartido, ya que esta contraseña nunca se transmite a través de la red.

La propiedad para el estado del servicio RADIUS está desactivada de forma predeterminada en Oracle ILOM. Para activar el estado del servicio RADIUS y configurar las propiedades de Oracle ILOM como cliente RADIUS, consulte la siguiente tabla.

TABLA 31 Configuración de Oracle ILOM para usar la autenticación del cliente/servidor LDAP

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/radius**
- **Web:** ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > RADIUS Settings (Configuración de RADIUS)
- **Rol de usuario:** User Management (u) (requerido para todas las modificaciones de propiedades)
- **Requisito:** el servidor RADIUS debe estar preconfigurado con los usuarios y la contraseña de tipo secreto compartido.

Propiedad	Valor predeterminado	Descripción
State (Estado) `(state=)`	Disabled (Desactivado)	*Disabled* |*Enabled* Para configurar Oracle ILOM como cliente RADIUS, establezca el estado de la propiedad State en activado. Cuando se activa la propiedad State, Oracle ILOM envía los datos de inicio de sesión de usuario al servidor RADIUS para la autenticación y autorización de usuarios. **Sintaxis de la CLI para estado de RADIUS**: **set /***SP*|*CMM***/clients/radius/ state=***disabled***|***enabled*

TABLA 31 Configuración de Oracle ILOM para usar la autenticación del cliente/servidor LDAP *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**clients/radius**
- **Web:** **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > RADIUS Settings (Configuración de RADIUS)**
- **Rol de usuario:** **User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito:** **el servidor RADIUS debe estar preconfigurado con los usuarios y la contraseña de tipo secreto compartido.**

Propiedad	Valor predeterminado	Descripción
Roles (`defaultrole=`)	Operator (Operador)	*Administrator* |*Operator* |*Advanced* Para definir qué funciones de Oracle ILOM estarán disponibles para los usuarios autenticados de RADIUS, establezca la propiedad Roles predeterminada en uno de los tres roles de usuario de Oracle ILOM: Administrator (a|u|c|r|o), Operator (c|r|o), Advanced (*a*|*u*|*c*|*r*|*o*|*s*). Los niveles de autorización para usar funciones dentro de Oracle ILOM están determinados por los privilegios otorgados por el rol de usuario configurado de Oracle ILOM. Para obtener una descripción de los privilegios asignados, consulte las tablas sobre roles de usuario y perfiles de usuario que se enumeran a continuación en la sección Información relacionada. **Sintaxis de la CLI para roles**: **set /***SP*|*CMM***/clients/radius/ defaultrole=***administrator***|***operator***|***a***|***u***|***c***|***r***|***o***|***s* **Información relacionada:** ■ Tabla 9 ■ Tabla 10
Address (Dirección) (`address=`)	0.0.0.0	*IP address*| *DNS host name* (servidor LDAP) Para configurar una dirección de red para el servidor RADIUS, complete la propiedad Address con la dirección IP del servidor RADIUS o el nombre de host DNS. Si se especifica un nombre de host DNS, las propiedades de configuración de DNS deberán estar definidas y activadas correctamente en Oracle ILOM. **Sintaxis de la CLI para dirección**: **set /***SP*|*CMM***/clients/radius/ address=***radius_server ip_address***|***ldap_server_dns_host_name* **Información relacionada:** ■ Tabla 44
Port (Puerto) (`port=`)	1812	*1812* | *User-specified TCP port* Oracle ILOM utiliza el puerto TCP 1812 para comunicarse con el servidor LDAP. Si es necesario, configure Oracle ILOM para que utilice otro puerto. Para ello, modifique el número de puerto predeterminado: 1812 **Sintaxis de la CLI para puerto**: **set /***SP*|*CMM***/clients/radius/ port=***number*

TABLA 31 Configuración de Oracle ILOM para usar la autenticación del cliente/servidor LDAP *(Continuación)*

Destino configurable de la interfaz de usuario:

- **CLI**: **/***SP***|***CMM***/clients/radius**
- **Web**: **ILOM Administration (Administración de ILOM) > User Management (Gestión de usuarios) > RADIUS Settings (Configuración de RADIUS)**
- **Rol de usuario: User Management (u) (requerido para todas las modificaciones de propiedades)**
- **Requisito: el servidor RADIUS debe estar preconfigurado con los usuarios y la contraseña de tipo secreto compartido.**

Propiedad	Valor predeterminado	Descripción
Shared Secret (Secreto compartido) (secret=)		Complete la propiedad Shared Secret con la contraseña compartida conocida del cliente/servidor RADIUS. El modelo del cliente/servidor RADIUS utiliza la contraseña compartida para su reconocimiento y para proteger los datos confidenciales de credenciales de usuario. **Sintaxis de la CLI para secreto compartido**: **set /***SP*|*CMM***/clients/radius/ secret=***password*
Save (Guardar)		**Interfaz web**. Para aplicar los cambios realizados en las propiedades dentro de la página RADIUS Settings (Configuración de RADIUS), debe hacer clic en Save (Guardar).

Modificación de la configuración predeterminada para la administración y la implementación de redes

Descripción	Vínculos
Consulte esta sección para comprender mejor las opciones de implementación de Oracle ILOM y la configuración predeterminada para el acceso de gestión y la conectividad de red.	■ "Principios y consideraciones para la implementación de red" en la página 82
Consulte esta sección si desea obtener información sobre los requisitos del acceso de gestión y las propiedades de la configuración.	■ "Modificación de las propiedades predeterminadas de configuración de acceso de gestión" en la página 92
Consulte esta sección si desea obtener información sobre los requisitos de conectividad y las propiedades de la configuración.	■ "Modificación de las propiedades predeterminadas de configuración de la conectividad" en la página 107
Consulte estas secciones si desea obtener instrucciones para configurar las etiquetas de identificación del sistema y definir las propiedades de fecha y hora en Oracle ILOM.	■ "Asignación de la información sobre identificación del sistema" en la página 121 ■ "Configuración de propiedades para el reloj del SP o el CMM " en la página 123
Consulte esta sección si desea obtener directrices para resolver problemas de acceso de gestión y conectividad de red.	■ "Resoluciones sugeridas para problemas de conectividad de red" en la página 125

Información relacionada

- *Guía de seguridad de Oracle ILOM 3.1*, consideraciones para la implementación
- *User?s Guide*, Logging In to Oracle ILOM

Principios y consideraciones para la implementación de red

Al configurar Oracle ILOM en una red, es importante comprender la configuración de red inicial que Oracle ILOM trae de fábrica, así como otras opciones configurables que los administradores de red pueden decidir implementar.

Si desea obtener información sobre las opciones de implementación de red para Oracle ILOM e información general para tener en cuenta al gestionar el entorno de red de Oracle ILOM, lea estos temas:

- "Opciones de implementación de acceso de gestión" en la página 83
- "Opciones de implementación de conectividad" en la página 86
- "Uso de certificados de servidor web y claves de servidor SSH" en la página 87
- "Tiempo de espera predeterminado para sesiones web y de la CLI" en la página 88
- "Visualización de mensajes de rótulo en el inicio de sesión" en la página 88
- "Formato de entrada para direcciones IPv4 e IPv6" en la página 89

- "Propietario del puerto de gestión serie" en la página 89
- "Puertos de red predeterminados utilizados por Oracle ILOM" en la página 89
- "Servidores Sun heredados no compatibles con IPv6" en la página 91

Opciones de implementación de acceso de gestión

Oracle ILOM admite la configuración de varios servicios de gestión de red. Algunos de estos servicios están activados de manera predeterminada, mientras que otros requieren configuración. Para comprender mejor cuáles son los servicios de gestión que vienen activados y cuáles son los que se necesitan realmente para su entorno de red, vea la siguiente tabla.

Nota – Active sólo los servicios de gestión que necesite en su entorno de gestión de red.

TABLA 32 Opciones y configuración predeterminada de la implementación del acceso de gestión

Acceso de gestión	Servicio de gestión	Valores predeterminados	Descripción
Cliente del explorador web	■ Servidor web	■ HTTPS sobre puerto 443 activado ■ TLSv1, activado ■ Certificado SSL y claves autofirmadas ■ Sesión de tiempo de espera de cliente, 15 minutos	De forma predeterminada, el servicio de gestión del servidor web en Oracle ILOM activa un canal de comunicación seguro entre un cliente del explorador web y el SP o el CMM de Oracle ILOM. Los administradores de la red pueden aceptar las propiedades predeterminadas del servidor web que se proporcionan en Oracle ILOM o pueden modificarlas según sea necesario. **Información relacionada**: ■ "Uso de certificados de servidor web y claves de servidor SSH" en la página 87 ■ Tabla 35 ■ "Resolución de configuraciones de seguridad de explorador web" en la página 125
Cliente SSH de la línea de comandos	■ Servidor de shell seguro (SSH)	■ Puerto 22 activado ■ Claves SSH generadas ■ Sesión de tiempo de espera de cliente, ilimitada	El servicio del servidor SSH en Oracle ILOM utiliza claves de servidor para cifrar el canal de gestión entre un cliente de la línea de comandos SSH y un SP o un CMM de Oracle ILOM. Oracle ILOM genera automáticamente las claves SSH de servidor cuando el sistema predeterminado de fábrica se inicia por primera vez. **Información relacionada**: ■ Tabla 38 ■ "Uso de certificados de servidor web y claves de servidor SSH" en la página 87

TABLA 32 Opciones y configuración predeterminada de la implementación del acceso de gestión *(Continuación)*

Acceso de gestión	Servicio de gestión	Valores predeterminados	Descripción
Cliente de aplicaciones SNMP	■ Protocolo simple de administración de redes (SNMP)	■ SNMPv3 sobre puerto 161, activado ■ Conjuntos de SNMP desactivado ■ Se requiere configuración de cuenta de usuario	El servicio de gestión de SNMP en Oracle ILOM ofrece una solución de gestión de protocolos segura para supervisar y gestionar los servidores de Oracle. Todas las funciones de supervisión y gestión de SNMP están disponibles desde una aplicación SNMP, por ejemplo, Net-SNMP. Antes de utilizar el servicio de gestión de SNMP en Oracle ILOM, se deben crear una o más cuentas de usuario de Oracle ILOM. Asimismo, antes de utilizar los conjuntos de SNMP, se debe activar la propiedad SNMP Sets. Oracle ILOM viene con SNMPv3 activado, pero los administradores pueden activar las propiedades de SNMPv1 o SNMPv2c si lo desean. **Información relacionada**: ■ Tabla 37 ■ *SNMP, IPMI, CIM, WS-MAN Protocol Management*, Configuring SNMP Settings in Oracle ILOM ■ “Propiedades de configuración de las notificaciones de alerta” en la página 178 ■ Net-SNMP (`http://net-snmp.sourceforge.net/`)

TABLA 32 Opciones y configuración predeterminada de la implementación del acceso de gestión *(Continuación)*

Acceso de gestión	Servicio de gestión	Valores predeterminados	Descripción
IPMItoolclient	■ IPMI	■ IPMPv2 sobre puerto 623, activado ■ Estado de servicio activado	El servicio de gestión de IPMI en Oracle ILOM ofrece una solución de protocolo seguro para supervisar y gestionar los servidores de Oracle. Las funciones de supervisión y gestión de IPMI están disponibles desde la CLI de Oracle ILOM mediante la utilidad IPMItool. Las propiedades configurables de IPMI en Oracle ILOM incluyen el estado del servicio de gestión de IPMI y los roles de usuario requeridos (Administrator [Administrador] u Operator [Operador]) para llevar a cabo las funciones de gestión de IPMI desde la CLI de Oracle ILOM. **Información relacionada**: ■ Tabla 39 ■ "Roles de usuario asignables de Oracle ILOM" en la página 40 ■ Referencia de gestión de protocolos de Oracle ILOM 3.1, Gestión de servidores con IPMI ■ "Propiedades de configuración de las notificaciones de alerta" en la página 178 ■ IPMItool (`http://ipmitool.sourceforge.net/`)

TABLA 32 Opciones y configuración predeterminada de la implementación del acceso de gestión *(Continuación)*

Acceso de gestión	Servicio de gestión	Valores predeterminados	Descripción
Cliente de gestión del servicio web	■ WS-Management (WS-Man)	■ HTTP[1] sobre puerto 8899 activado ■ Estado de servicio activado	El servicio de WS-Management en Oracle ILOM ofrece una interfaz de servicio web estándar para: ■ Supervisión del estado de los servidores de Oracle ■ Generación de informes del estado de inventario ■ Gestión remota de la energía en un servidor host ■ Restablecimiento remoto del SP de Oracle ILOM Las opciones configurables de WS-Man en Oracle ILOM incluyen el modo de protocolo de transferencia (HTTP o HTTPS), el puerto de comunicación (8899 u 8888) y el estado del servicio. Los administradores de la red pueden aceptar las propiedades predeterminadas de WS-Man que se proporcionan en Oracle ILOM o pueden modificarlas según sea necesario. **Información relacionada**: ■ "Uso de certificados de servidor web y claves de servidor SSH" en la página 87 ■ Tabla 41 ■ *SNMP, IPMI, CIM, WS-MAN Protocol Management*, Server Management Using WS-Management and CIM

[1] Para maximizar la seguridad, el modo de protocolo de transferencia preferido es HTTPS sobre puerto 8888.

Opciones de implementación de conectividad

Las opciones de conectividad de Oracle ILOM vienen preconfiguradas para que Oracle ILOM pueda obtener la dirección de red del SP o del CMM del servidor físico. Para comprender mejor cuáles son las propiedades de conectividad que vienen activadas y cuáles son las que se necesitan para su entorno de red, vea la siguiente tabla.

TABLA 33 Opciones de implementación y configuración predeterminada de la conectividad

Opciones de conectividad	Valores predeterminados	Descripción
Red	■ IPv 4, DHCP activado ■ IP 6, sin estado activado ■ Puerto de gestión: MGT	De forma predeterminada, Oracle ILOM viene configurado para funcionar en un entorno de red de IPv4 e IPv6 de doble pila. Cuando se configura una conexión de gestión de red física con el servidor o el CMM, Oracle ILOM intenta obtener la dirección física del SP o el CMM de los dispositivos de enrutamiento o asignación de IP configurados en la red. Los administradores de la red pueden aceptar las propiedades de red IP de doble pila predeterminadas de Oracle ILOM o pueden desactivarlas y configurar las propiedades de red IP que sean necesarias. **Información relacionada**: ■ Tabla 43 ■ "Conexión de gestión de red de banda lateral" en la página 15 ■ "Conexión de gestión de red dedicada (predeterminado)" en la página 12
DNS	■ DNS automático por medio de DHCP, activado ■ Tiempo de espera de DNS, 5 segundos ■ Reintentos de DNS, 1	La propiedad Auto DNS (DNS automático) de Oracle ILOM utiliza DHCP para asignar automáticamente el servidor de nombres y la ruta de búsqueda del DNS. Los administradores de la red pueden aceptar las propiedades predeterminadas del DNS automático de Oracle ILOM o pueden desactivarlas y configurar el servidor de nombres y la ruta de búsqueda del DNS requeridos. **Información relacionada**: ■ Tabla 44 ■ "Configuración de ejemplo de DNS dinámico" en la página 119
Puertos serie	■ Propietario = SP ■ Velocidad en baudios: = 9600 ■ Control de flujo = ninguno	La función de salida de la consola para el puerto de gestión serie físico del servidor está controlada por el SP del servidor. Los administradores de la red pueden aceptar el SP del servidor como propietario predeterminado del puerto serie o pueden transferir la propiedad del puerto al sistema operativo del servidor host. **Información relacionada**: ■ Tabla 45 ■ "Propietario del puerto de gestión serie" en la página 89 ■ "Conexión de gestión de red dedicada (predeterminado)" en la página 12

Uso de certificados de servidor web y claves de servidor SSH

Oracle ILOM viene preconfigurado con un certificado autofirmado de servidor web y un conjunto de claves de servidor SSH generadas, lo que permite a Oracle ILOM garantizar la autenticidad de un servidor o un cliente.

Los administradores de la red pueden elegir utilizar el certificado de servidor web autofirmado listo para usar o, si lo desean, pueden cargar un certificado de servidor web firmado en Oracle ILOM. Asimismo, las claves de servidor SSH generadas se pueden volver a generar según sea necesario.

Si desea obtener información detallada sobre las propiedades de configuración del certificado del servidor web, consulte Tabla 36.

Si desea obtener información detallada sobre las propiedades de configuración de las claves de servidor SSH, consulte Tabla 38.

Tiempo de espera predeterminado para sesiones web y de la CLI

Oracle ILOM proporciona propiedades configurables que controlan la cantidad de minutos que puede estar inactivo un cliente web o de línea de comandos antes de que Oracle ILOM finalice la sesión.

La sesión de tiempo de espera predeterminada para los usuarios web autorizados es de 15 minutos, mientras que la sesión de tiempo de espera predeterminada para usuarios de línea de comandos autorizados es de 0 minutos (lo que significa que no hay un tiempo de espera predeterminado configurado para la CLI). Para impedir el uso no autorizado de una sesión que no esté supervisada, debe configurar un tiempo de espera adecuado para todos los usuarios web y de la CLI.

Para obtener información sobre las propiedades de configuración del tiempo de espera de las sesiones de la CLI, consulte Tabla 40. Para obtener información sobre las propiedades de configuración del tiempo de espera de las sesiones web, consulte Tabla 35.

Visualización de mensajes de rótulo en el inicio de sesión

Las propiedades de los mensajes de rótulo de Oracle ILOM permiten a los administradores de la red presentar mensajes importantes a los usuarios de Oracle ILOM cuando inician sesión. Por ejemplo, los administradores de la red pueden utilizar esta función de presentación de mensajes para alertar a los usuarios acerca de restricciones de acceso especiales, generar avisos de actividades de mantenimiento futuras en el sistema y otros propósitos similares.

Los mensajes de rótulo de la interfaz web y de la CLI de Oracle ILOM pueden aparecer antes de que el usuario inicie sesión o inmediatamente después de que lo haga. Para configurar un mensaje de rótulo y activarlo, consulte Tabla 42.

Formato de entrada para direcciones IPv4 e IPv6

Oracle ILOM acepta el siguiente formato de entrada para direcciones IPv4 e IPv6.

Dirección	Formato de entrada
IPv4 (32 bits)	Cuatro números separados con punto: *n.n.n.n* **Ejemplo**: 192.0.2.0
IPv6 (128 bits)	Al introducir una dirección IPv6 o una dirección IPv6 local de vínculo, la dirección debe ir entre corchetes para que funcione correctamente. Sin embargo, al especificar una dirección IPv6 para iniciar sesión en Oracle ILOM con SSH, no escriba la dirección IPv6 entre corchetes. **Ejemplos**: ■ Dirección IPv6: [2001:db8:0:0:0:0:0:0/32] ■ Dirección IPv6 con SSH y cuenta `root`: ssh root@2001:db8:0:0:0:0:0:0/32 ■ Dirección IPv6 local de vínculo: [fe80::214:4fff:feca:5f7e/64]

Propietario del puerto de gestión serie

En todos los servidores de Oracle que tienen Oracle ILOM, la salida del puerto SER MGT está configurada para el SP del servidor. Sin embargo, en algunos servidores de Oracle, Oracle ILOM proporciona una propiedad que permite a los administradores de la red transferir la propiedad del puerto serie entre el SP del servidor (configuración predeterminada) y el sistema operativo del servidor host.

Cuando el propietario del puerto serie se transfiere al servidor host, el sistema operativo host controla las funciones del puerto serie y el SP del servidor no tiene control sobre el puerto serie ni acceso a él.

Antes de transferir la propiedad del puerto serie al servidor host, los administradores de la red deben asegurarse de que se haya establecido una conexión de gestión de red con el SP del servidor. De no ser así, es decir, si no se estableció una conexión de gestión de red y el servidor host está establecido como propietario del puerto serie, ningún usuario podrá tener acceso local ni remoto al SP de Oracle ILOM.

Para modificar la propiedad predeterminada de propietario del puerto serie en Oracle ILOM, consulte Tabla 45.

Puertos de red predeterminados utilizados por Oracle ILOM

Consulte la siguiente tabla para determinar cuáles son los puertos red utilizados por Oracle ILOM de forma predeterminada (listos para usar):

TABLA 34 Puertos de red predeterminados de Oracle ILOM

Puerto	Protocolo	Aplicación
Puertos de red comunes		
22	SSH sobre TCP	SSH: shell seguro
25	SMPT sobre TCP	Comunicación de cliente SMPT
69	TFTP sobre UDP	TFTP: protocolo trivial de transferencia de archivos (de salida)
80	HTTP sobre TCP	Web (configurable por el usuario)
123	NTP sobre UDP	NTP: protocolo de hora de red (de salida)
161	SNMP sobre UDP	SNMP: protocolo simple de administración de redes (configurable por el usuario)
162	IPMI sobre UDP	IPMI: captura de eventos de plataforma (PET) (de salida)
389	LDAP sobre UDP/TCP	LDAP: protocolo ligero de acceso a directorios (de salida; configurable por el usuario)
443	HTTPS sobre TCP	Web (configurable por el usuario)
514	Syslog sobre UDP	Syslog (de salida)
623	IPMI sobre UDP	IPMI: interfaz inteligente de gestión de plataformas
546	DHCP sobre UDP	DHCP: protocolo de configuración dinámica de host (cliente)
1812	RADIUS sobre UDP	RADIUS: servicio de autenticación remota telefónica de usuario (de salida; configurable por el usuario)
8888	WS-Man sobre HTTP	Servicio de WS-Man
8889	WS-Man sobre HTTPS	Servicio de WS-Man
Puertos de red de SP		
5120	TCP	Oracle ILOM Remote Console: CD
5121	TCP	Oracle ILOM Remote Console: teclado y mouse
5123	TCP	Oracle ILOM Remote Console: disquete
5555	TCP	Oracle ILOM Remote Console: cifrado
5556	TCP	Oracle ILOM Remote Console: autenticación
6481	TCP	Oracle ILOM Remote Console: daemon Servicetag
7578	TCP	Oracle ILOM Remote Console: video
7579	TCP	Oracle ILOM Remote Console: serie

TABLA 34 Puertos de red predeterminados de Oracle ILOM *(Continuación)*

Puerto	Protocolo	Aplicación
Puertos de red de CMM		
8000 - 8023	HTTP sobre TCP	Búsqueda detallada de módulos de servidor (blades) de Oracle ILOM
8400 - 8423	HTTPS sobre TCP	Búsqueda detallada de módulos de servidor (blades) de Oracle ILOM
8200 - 8219	HTTP sobre TCP	Búsqueda detallada de módulos de ampliación de red de Oracle ILOM
8600 - 8619	HTTPS sobre TCP	Búsqueda detallada de módulos de ampliación de red de Oracle ILOM

Servidores Sun heredados no compatibles con IPv6

Si desea ver una lista de los SP de servidores Sun heredados que actualmente no admiten IPv6, consulte la siguiente tabla.

Plataforma Sun	Modelo de servidor
SPARC Enterprise	■ T5440 ■ T5220 ■ T5120 ■ T5140 ■ T5240 ■ T6340
x86 Sun Fire	■ X4140 ■ X4150 ■ X4240 ■ X4440 ■ X4450 ■ X4600 ■ X4600 M2 ■ X4640

Modificación de las propiedades predeterminadas de configuración de acceso de gestión

Los administradores de la red pueden aceptar o modificar las propiedades predeterminadas de acceso de gestión de Oracle ILOM. Para modificar las propiedades predeterminadas de acceso de gestión de Oracle ILOM, consulte las siguientes tablas:

- Tabla 35
- Tabla 36
- Tabla 37
- Tabla 38
- Tabla 39
- Tabla 40
- Tabla 41
- Tabla 42

TABLA 35 Propiedades de configuración de servidores web

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/*services*/
- **Web:** ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > Web Server (Servidor web) > Web Server Settings (Configuración de servidor web)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Propiedad	Valor predeterminado	Descripción
HTTP Webserver (Servidor web HTTP) (`http/ securedirect=enabled servicestate=disabled`)	Redirect Connection to HTTPS (Redirigir conexión a HTTPS)	*Redirect Connection to HTTPS* |*Enabled* |*Disabled* Cuando la propiedad HTTP Webserver está establecida en Redirect Connection to HTTPS, la propiedad del estado del servicio del servidor web HTTPS se activa automáticamente. Estos valores predeterminados de la propiedad indican a Oracle ILOM que utilice HTTPS para transmitir información de manera segura al servidor web. Cuando la propiedad HTTP Webserver está activada, Oracle ILOM utiliza HTTP, que es un protocolo no cifrado, para transmitir información al servidor web. Cuando la propiedad HTTP Webserver está desactivada, el uso de la transmisión de información al servidor web por HTTP está desactivado en Oracle ILOM. **Sintaxis de la CLI para el servidor web HTTP**: **set /***SP*|*CMM***/services/http securedirect=***enabled*|*disabled* **servicestate=***disabled*|*enabled*

TABLA 35 Propiedades de configuración de servidores web *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI:** /*SP*|*CMM/services/*
- **Web:** **ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > Web Server (Servidor web) > Web Server Settings (Configuración de servidor web)**
- **Rol de usuario: admin (a) (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
HTTP Port (Puerto HTTP) (`http/ port=`)	80	*80* |*User_defined* Cuando está activado el estado del servicio HTTP, Oracle ILOM se comunica de forma predeterminada con el servidor web mediante HTTP sobre el puerto TCP 80. Si es necesario, el número de puerto predeterminado se puede cambiar. **Sintaxis de la CLI para el puerto HTTP**: **`set /`***SP*|*CMM***`/services/http port=<`***n***`>`**
HTTP Session Timeout (Tiempo de espera de sesión HTTP) (`http/ sessiontimeout=`)	15 seconds (15 segundos)	*15 seconds* |*User_defined* El tiempo de espera de la sesión web HTTP determina la cantidad de minutos que transcurren hasta que se cierra automáticamente la sesión de un cliente de explorador web inactivo. El tiempo de espera de sesión web HTTP predeterminado es de 15 minutos. Si es necesario, el valor predeterminado del tiempo de espera de sesión se puede aumentar o reducir. **Sintaxis de la CLI para el tiempo de espera de sesiones HTTP**: **`set /`***SP*|*CMM***`/services/http sessiontimeout=<`***n***`>`**
HTTPS Webserver (Servidor web HTTPS) (`https/ servicestate=enabled`)	Enabled (Activado)	*Enabled* |*Disabled* Cuando la propiedad HTTPS Webserver está activada, Oracle ILOM utiliza HTTPS para transmitir información al servidor web de manera segura. Cuando la propiedad HTTPS Webserver está desactivada, el uso de la transmisión de información al servidor web por HTTPS está desactivado en Oracle ILOM. **Sintaxis de la CLI para el servidor web HTTPS**: **`set /`***SP*|*CMM***`/services/https servicestate=`***enabled*|*disabled*
HTTPS Port (Puerto HTTPS) (`https/ port=`)	443	*443* |*User_defined* Cuando está activado el estado del servicio HTTPS, Oracle ILOM se comunica de forma predeterminada con el servidor web mediante HTTPS sobre el puerto TCP 443. Si es necesario, el número de puerto predeterminado se puede cambiar. **Sintaxis de la CLI para el puerto HTTPS**: **`set /`***SP*|*CMM***`/services/https port=<n>`**

TABLA 35 Propiedades de configuración de servidores web *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM/services/*
- **Web: ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > Web Server (Servidor web) > Web Server Settings (Configuración de servidor web)**
- **Rol de usuario: admin (a) (requerido para todas las modificaciones de propiedades)**

<table>
<tr><th>Propiedad</th><th>Valor predeterminado</th><th>Descripción</th></tr>
<tr><td>HTTPS Session Timeout (Tiempo de espera de sesión HTTPS)

(https/sessiontimeout=)</td><td>15 seconds (15 segundos)</td><td><i>15 seconds |User_defined</i>

El tiempo de espera de la sesión web HTTPS determina la cantidad de minutos que transcurren hasta que se cierra automáticamente la sesión de un cliente de explorador web inactivo. El tiempo de espera de sesión web HTTPS predeterminado es de 15 minutos. Si es necesario, el valor predeterminado del tiempo de espera de sesión se puede aumentar o reducir.

Sintaxis de la CLI para el tiempo de espera de sesiones HTTPS:

set /<i>SP</i>|<i>CMM</i>/services/https sessiontimeout=<<i>n</i>></td></tr>
<tr><td>SSLv2 (https/ sslv2=disabled)</td><td>Disabled (Desactivado)</td><td>Disabled |Enabled

La propiedad SSLv2 está desactivada de forma predeterminada. Si es necesario, la propiedad SSLv2 predeterminada se puede activar.

Sintaxis de la CLI para SSLv2:

set /SP|CMM/services/https sslv2=disabled|enabled</td></tr>
<tr><td>SSLv3 (https/ sslv3=enabled)</td><td>Enabled (Activado)</td><td>Enabled |Disabled

De forma predeterminada, Oracle ILOM utiliza SSLv3 y TLSv1 para activar el cifrado más potente de la capa de conexión segura. Si es necesario, la propiedad SSLv3 predeterminada se puede desactivar.

Sintaxis de la CLI para SSLv3:

set /SP|CMM/services/https sslv3=enabled|disabled</td></tr>
<tr><td>TLSv1 (https/ tlsv1=enabled)</td><td>Enabled (Activado)</td><td>Enabled |Disabled

De forma predeterminada, Oracle ILOM utiliza SSLv3 y TLSv1 para activar el cifrado más potente de la capa de conexión segura. Si es necesario, la propiedad TLSv1 predeterminada se puede desactivar.

Sintaxis de la CLI para TLSv1:

set /SP|CMM/services/https tlsv1=enabled|disabled</td></tr>
</table>

TABLA 35 Propiedades de configuración de servidores web *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP|CMM/services/*
- **Web:** ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > Web Server (Servidor web) > Web Server Settings (Configuración de servidor web)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Propiedad	Valor predeterminado	Descripción
Weak Ciphers (Codificadores débiles) (`https/weak_ciphers=disabled`)	Disabled (Desactivado)	*Disabled |Enabled* La propiedad Weak Ciphers está desactivada de forma predeterminada. Puede ser necesario activarla para admitir el uso de exploradores web anteriores. **Sintaxis de la CLI para los codificadores débiles**: **set /***SP|CMM***/services/https weak_ciphers=***disabled|enabled* **Información relacionada**: ■ "Resolución de configuraciones de seguridad de explorador web" en la página 125
Save (Guardar)		**Interfaz web**: para aplicar los cambios hechos a las propiedades desde la página Web Server Settings (Configuración de servidor web), debe hacer clic en Save (Guardar).

TABLA 36 Propiedades de configuración del certificado SSL y las claves privadas para el servidor web HTTPS

Destino, rol de usuario y requisito de certificado SSL configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**services/https/ssl**
- **Web: ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > SSL Certificate (Certificado SSL) > SSL Certificate Upload (Carga de certificado SSL)**
- **Rol de usuario: admin (a) (requerido para todas las modificaciones de propiedades)**
- **Requisito: para una configuración personalizada válida de SSL, se necesita cargar tanto el certificado personalizado como una clave privada personalizada.**

Propiedad	Valor predeterminado	Descripción
Certificate File Status (Estado de archivo de certificado) `(certstatus=)`	Using Default (Usar valor predeterminado) (no hay un certificado o una clave privada personalizados cargados)	*Default_Certificate* |*Custom_Certificate* La propiedad Certificate Status es de sólo lectura. Esta propiedad indica cuál de los siguientes tipos de certificados SSL está actualmente en uso en el servidor web HTTPS: ■ Certificado SSL y clave autofirmada privada predeterminados proporcionados con Oracle ILOM O bien: ■ Certificado SSL de confianza y clave privada personalizados proporcionados por una autoridad de certificación de confianza **Nota**: Cuando se utiliza el certificado SSL predeterminado, se notifica a los usuarios que se conectan a la interfaz web de Oracle ILOM por primera vez que se está utilizando el certificado autofirmado predeterminado y se les solicita que acepten su uso. El certificado SSL autofirmado predeterminado garantiza que todas las comunicaciones entre los clientes del explorador web y el SP (o el CMM) de Oracle ILOM estén totalmente cifradas. **Sintaxis de la CLI para mostrar el estado del certificado**: **show /**/*SP*|*CMM*/**https/ssl**
Custom Certificate Load (Carga de certificado personalizado) `(/custom_certificate)`		**Interfaz web**: haga clic en el botón Load Certificate (Cargar certificado) para cargar el archivo de certificado personalizado designado en las propiedades del método de transferencia de archivos. **Nota**: Para una configuración de certificado personalizado válido, se necesita cargar un certificado personalizado y una clave privada personalizada. Sólo así el certificado SSL personalizado se aplicará y se mantendrá tras los reinicios del sistema y las operaciones de copia de seguridad y restauración. **Sintaxis de la CLI para cargar un certificado personalizado**: **load_uri=***file_transfer_method***://***host_address***/***file_path***/***custom_certificate_filename* Donde *file_transfer_method* puede incluir: *Browser*|*TFTP*|*FTP*|*SCP*|HTTP |HTTPS|*Paste* Si desea leer una descripción detallada de cada método de transferencia de archivos (excluido Paste [Pegar]), consulte "Métodos de transferencia de archivos admitidos" en la página 45.

TABLA 36 Propiedades de configuración del certificado SSL y las claves privadas para el servidor web HTTPS *(Continuación)*

Destino, rol de usuario y requisito de certificado SSL configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**services/https/ssl**
- **Web:** ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > SSL Certificate (Certificado SSL) > SSL Certificate Upload (Carga de certificado SSL)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)
- **Requisito:** para una configuración personalizada válida de SSL, se necesita cargar tanto el certificado personalizado como una clave privada personalizada.

Propiedad	Valor predeterminado	Descripción
Custom Certificate Remove (Eliminación de certificado personalizado) (`/custom_certicate clear_action=true`)		**Interfaz web**: haga clic en el botón Remove Certificate (Eliminar certificado) para eliminar el archivo de certificado SSL personalizado actualmente almacenado en Oracle ILOM. Cuando se le solicite confirmación, haga clic en Yes (Sí) para eliminarlo o No para cancelar la acción. **Sintaxis de la CLI para eliminar un certificado**: **set** /*SP*|*CMM*/**services/https/ssl/custom_certificate clear_action=true** Cuando se le solicite confirmación, escriba y para eliminarlo o `n` para cancelar la acción.
Custom Private Key (Clave privada personalizada) (`/custom_key`)		**Interfaz web**: haga clic en el botón Load Custom Private Key (Cargar clave privada personalizada) para cargar el archivo de clave privada personalizada designado en las propiedades del método de transferencia de archivos. **Nota**: Para una configuración de certificado personalizado válido, se necesita cargar un certificado personalizado y una clave privada personalizada. Sólo así el certificado SSL personalizado se aplicará y se mantendrá tras los reinicios del sistema y las operaciones de copia de seguridad y restauración. **Sintaxis de la CLI para cargar una clave privada personalizada**: **load_uri=***file_transfer_method***://***host_address***/***file_path***/***custom_key_filename* Donde *file_transfer_method* puede incluir: *Browser*|*TFTP*|*FTP*|*SCP*|HTTP |HTTPS|*Paste* Si desea leer una descripción detallada de cada método de transferencia de archivos (excluido Paste [Pegar]), consulte "Métodos de transferencia de archivos admitidos" en la página 45.
Custom Private Key Remove (Eliminación de clave privada personalizada) (`/custom_key clear_action=true`)		**Interfaz web**: haga clic en el botón Remove Custom Private Key (Eliminar clave privada personalizada) para eliminar el archivo de clave privada personalizada actualmente almacenado en Oracle ILOM. Cuando se le solicite confirmación, haga clic en Yes (Sí) para eliminarlo o No para cancelar la acción. **Sintaxis de la CLI para eliminar una clave privada de certificado**: **set** /*SP*|*CMM*/**services/https/ssl/custom_key clear_action=true** Cuando se le solicite confirmación, escriba y para suprimirlo `n` para cancelar la acción.

TABLA 37 Propiedades de configuración de SNMP

Destino, rol de usuario y requisito de SNMP configurables de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/**services/snmp**
- **Web**: **ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > SNMP > SNMP Management (Gestión de SNMP)**
- **Rol de usuario**: **admin (a) (requerido para todas las modificaciones de propiedades)**
- **Requisito**: **para el servicio SNMPv3, se necesitan cuentas de usuario; para los servicios SNMPv1 y v2c, se necesitan comunidades.**

Propiedad	Valor predeterminado	Descripción
State (Estado) (`state=`)	Enabled (Activado)	*Enabled* |*Disabled* El estado de SNMP está activado de forma predeterminada. Cuando esta propiedad está activada y las propiedades de una o más cuentas de usuario o comunidades para SNMP están configuradas, el servicio de gestión de SNMP de Oracle ILOM está disponible para utilizarse. Si la propiedad State de SNMP está desactivada, el puerto de SNMP se bloquea, lo que impide toda comunicación de SNMP entre Oracle ILOM y la red. **Sintaxis de la CLI para el estado de SNMP**: **set /***SP*|*CMM***/services/snmp state=***enabled*|*disabled*
Port (Puerto) (`port=`)	161	*161 | User_specified.* De forma predeterminada, Oracle ILOM utiliza el puerto TCP 161 para transmitir las comunicaciones de SNMP entre los SP de Oracle ILOM (o los CMM de Oracle ILOM) y la red. Si es necesario, el número predeterminado de la propiedad de puerto se puede cambiar. **Sintaxis de la CLI para el puerto SNMP**: **set /***SP*|*CMM***/services/snmp port=***n*
Engine ID (ID de motor) (engineid=)	Auto-set by SNMP agent (Configurado automáticamente por el agente de SNMP)	El agente de SNMP de Oracle ILOM establece automáticamente la propiedad Engine ID. Este ID es exclusivo para cada sistema compatible con SNMP de Oracle ILOM. Si bien Engine ID se puede configurar, siempre debe ser exclusivo de cada sistema de Oracle ILOM en todo el centro de datos. Sólo los usuarios de SNMP con experiencia y que estén familiarizados con la seguridad de SNMP v3 deben modificar la propiedad Engine ID de SNMP.

TABLA 37 Propiedades de configuración de SNMP *(Continuación)*

Destino, rol de usuario y requisito de SNMP configurables de la interfaz de usuario:

- **CLI**: */SP*|*CMM*/services/snmp
- **Web**: **ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > SNMP > SNMP Management (Gestión de SNMP)**
- **Rol de usuario**: **admin (a) (requerido para todas las modificaciones de propiedades)**
- **Requisito**: **para el servicio SNMPv3, se necesitan cuentas de usuario; para los servicios SNMPv1 y v2c, se necesitan comunidades.**

Propiedad	Valor predeterminado	Descripción
Set Requests (Establecer solicitudes) (sets=)	Disabled (Desactivado)	*Disabled* |*Enabled* La propiedad Set Requests está desactivada de forma predeterminada en Oracle ILOM. Cuando la propiedad Set Requests está desactivada, las siguientes MIB de SNMP están disponibles con fines de supervisión: ■ SUN-HW-TRAP-MIB: utilice esta MIB para supervisar notificaciones de capturas para hardware, por ejemplo, fallos de hardware. ■ SUN-PLATFORM-MIB: utilice esta MIB para sondear información relacionada con el hardware, por ejemplo, inventario y estado. Cuando la propiedad Set Requests está activada, las MIB descritas anteriormente están disponibles con fines de supervisión y las siguientes MIB están disponibles con fines de gestión: ■ SUN-HW-CTRL-MIB: utilice esta MIB para configurar políticas de hardware, por ejemplo, gestión de energía. ■ SUN-ILOM-CONTROL-MIB: utilice esta MIB para configurar funciones de Oracle ILOM, por ejemplo, crear usuarios y configurar servicios. **Sintaxis de la CLI para establecer solicitudes**: `set /SP|CMM/services/snmp sets=`*disabled*|*enabled* **Información relacionada**: ■ Referencia de gestión de protocolos de Oracle ILOM 3.1, Gestión de servidores con SNMP

TABLA 37 Propiedades de configuración de SNMP *(Continuación)*

Destino, rol de usuario y requisito de SNMP configurables de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/services/snmp
- **Web**: ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > SNMP > SNMP Management (Gestión de SNMP)
- **Rol de usuario**: admin (a) (requerido para todas las modificaciones de propiedades)
- **Requisito**: para el servicio SNMPv3, se necesitan cuentas de usuario; para los servicios SNMPv1 y v2c, se necesitan comunidades.

Propiedad	Valor predeterminado	Descripción
Protocols (Protocolos) (v1|v2c|v3)	v3, activado	*v1*|*v2c*|*v3* De forma predeterminada, Oracle ILOM activa el uso de SNMP v3 y desactiva el uso de SNMP v1 y v2c. SNMPv1 y v2c no admiten el cifrado y utilizan cadenas de comunidad como forma de autenticación. SNMPv3 utiliza cifrado para proporcionar un canal seguro y utiliza nombres de usuario y contraseñas individuales que se almacenan de manera segura en la estación de gestión de SNMP. Si es necesario, el valor predeterminado de la propiedad Protocols de SNMP se puede configurar. **Nota –** Use SNMP v2c o v3 para supervisión y mantenga la propiedad predeterminada desactivada para Set Requests. **Sintaxis de la CLI para modificar el protocolo predeterminado**: **set /SP|CMM/services/snmp** *v1*|*v2c*|*v3*=*enabled*|*disabled*
Save (Guardar)		**Interfaz web**: para aplicar los cambios hechos a las propiedades desde la página SNMP Management (Gestión de SNMP), debe hacer clic en Save (Guardar).
SNMP Communities (Comunidades de SNMP) (/communities)		*Community Name* |*Permission= Read-only* (ro)| *Read-write* (rw) Las comunidades de SNMP se utilizan solamente con SNMP v1 o v2c para controlar el acceso de los usuarios y los niveles de autorización en Oracle ILOM. Cuando la propiedad Protocols de SNMP v1 o v2c está activada, se pueden configurar las propiedades de comunidades de SNMP en Oracle ILOM. Al configurar las comunidades, se aplican las siguientes reglas: ■ Nombre de la comunidad: hasta 35 caracteres de longitud, debe comenzar con un carácter alfabético y no puede contener espacios. ■ Guardar (sólo interfaz web): todos los cambios hechos desde el cuadro de diálogo Add SNMP User (Agregar usuario de SNMP) de SNMP se deben guardar. **Sintaxis de la CLI para crear comunidades de SNMP**: **create /***SP*|*CMM***/services/snmp/communities name=***community_name* **permission=***rw*|*ro* **show /***SP*|*CMM***/services/snmp/communities** *public*|*private* **delete /***SP*|*CMM***/services/snmp/communities** *community_name*

TABLA 37 Propiedades de configuración de SNMP *(Continuación)*

Destino, rol de usuario y requisito de SNMP configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/services/snmp
- **Web:** ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > SNMP > SNMP Management (Gestión de SNMP)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)
- **Requisito:** para el servicio SNMPv3, se necesitan cuentas de usuario; para los servicios SNMPv1 y v2c, se necesitan comunidades.

Propiedad	Valor predeterminado	Descripción
SNMP Users (Usuarios de SNMP) (`/users`)		*Username* | *Authentication Password* | *Permission*| *Authentication Protocol* | *Privacy Protocol* Los usuarios de SNMP se utilizan solamente con SNMP v3 para controlar el acceso de los usuarios y los niveles de autorización en Oracle ILOM. Cuando la propiedad Protocols de SNMP v3 está activada, se pueden configurar las propiedades de usuarios de SNMP en Oracle ILOM. Al configurar los usuarios de SNMP, se aplican las siguientes reglas: ■ Nombre de usuario: hasta 35 caracteres de longitud, debe comenzar con un carácter alfabético y no puede contener espacios. ■ Autenticación o contraseña de privacidad: hasta 16 caracteres de longitud, distingue mayúsculas de minúsculas, sin espacios ni signos de dos puntos, y se debe confirmar la contraseña. ■ Guardar (sólo interfaz web): todos los cambios hechos desde el cuadro de diálogo Add SNMP User (Agregar usuario de SNMP) de SNMP se deben guardar. **Sintaxis de la CLI para crear usuarios de SNMP**: **create /***SP*|*CMM***/services/snmp/users username=***value* **authenticationprotocol=***MD5*|*SHA* **authenticationpassword=***value* **permissions=ro|rw privacyprotocol=***aes*|*des*|*none* **show /***SP*|*CMM***/services/snmp/users** **delete /***SP*|*CMM***/services/snmp/username**
MIBs Download (Descarga de MIB) (`/mibs dump_uri=`)		Oracle ILOM permite descargar las MIB del SNMP de SUN directamente del SP del servidor o el CMM.

TABLA 38 Propiedades de configuración de servidores SSH

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**services/ssh**
- **Web: ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > SSH Server (Servidor SSH) > Web Server Settings (Configuración de servidor SSH)**
- **Rol de usuario: admin (a) (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
State (Estado) (`state=`)	Enabled (Activado)	*Enabled* |*Disabled* La propiedad State del servidor SSH está activada de forma predeterminada. Cuando la propiedad State del servidor SSH está activada, el servidor SSH utiliza claves de servidor para permitir a los clientes remotos conectarse de manera segura con el SP de Oracle ILOM (o el CMM de Oracle ILOM) desde la interfaz de línea de comandos. Cuando la propiedad State del servidor SSH se desactiva o se reinicia, se finalizan automáticamente todas las sesiones del SP o el CMM de la CLI que se estén ejecutando sobre SSH. **Nota**: Oracle ILOM genera automáticamente las claves de servidor SSH cuando el sistema predeterminado de fábrica se inicia por primera vez. **Interfaz web**: para que los cambios hechos en el estado del servidor SSH desde la interfaz web tengan efecto en Oracle ILOM, debe hacer clic en Save (Guardar). **Sintaxis de la CLI para el estado del servidor SSH**: **set /***SP*|*CMM***/services/ssh state=***enabled*|*disabled*
Botón Restart (Reiniciar) (`restart_sshd_action=`)		*True*|*False* Cuando se reinicia el servidor SSH, se producen automáticamente las siguientes acciones: (1) se finalizan todas las sesiones de la CLI del SP o el CMM conectadas y (2) se activan nuevas claves de servidor pendientes. **Sintaxis de la CLI para reiniciar**: **set /***SP*|*CMM***/services/ssh restart_sshd_action=true**
Botón Generate RSA Key (Generar clave RSA) (`generate_new_key_type=rsa generate_new_key_action= true`)		Permite generar una nueva clave RSA de SSH. **Sintaxis de la CLI para generar claves RSA**: **set /***SP*|*CMM***/services/ssh generate_new_key_type=rsa generate_new_key_action=true**

TABLA 38 Propiedades de configuración de servidores SSH *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**services/ssh**
- **Web:** ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > SSH Server (Servidor SSH) > Web Server Settings (Configuración de servidor SSH)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Propiedad	Valor predeterminado	Descripción
Botón Generate DSA Key (Generar clave DSA) (`generate_new_key_type=dsa generate_new_key_action=`)		Permite generar una nueva clave DSA de SSH. **Sintaxis de la CLI para generar claves DSA:** **set /***SP*|*CMM***/services/ssh generate_new_key_type=dsa generate_new_key_action=true**

TABLA 39 Propiedades de configuración del servicio de IPMI

Destino configurable de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**services/ipmi**
- **Web:** ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > IPMI > IPMI Settings (Configuración de IPMI)

Roles de usuario:

- admin (a): requerido para las modificaciones de propiedades de configuración de especificaciones de IPMI
- Administrator u Operator: requerido al utilizar el servicio de IPMI (IPMItool) desde la CLI de Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
State (Estado) (`state=`)	Enabled (Activado)	*Enabled* |*Disabled* La propiedad State de IPMI v2 está activada de forma predeterminada. Cuando la propiedad State de IPMI está activada, Oracle ILOM permite a los clientes remotos de IPMItool conectarse de manera segura con el SP de Oracle ILOM (o el CMM de Oracle ILOM) mediante la interfaz de línea de comandos. Cuando la propiedad State de IPMI se desactiva, todos los clientes de IPMItool conectados al SP o el CMM por medio de la CLI de Oracle ILOM se desconectan automáticamente. **Interfaz web**: para que los cambios hechos en el estado de IPMI desde la interfaz web tengan efecto en Oracle ILOM, debe hacer clic en Save (Guardar). **Sintaxis de la CLI para el estado de IPMI**: **set /***SP*|*CMM***/services/ipmi state=enabled|disabled**

TABLA 40 Propiedad de configuración del tiempo de espera de las sesiones de la CLI

Destino configurable de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/**cli**
- **Web**: **ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > IPMI > IPMI Settings (Configuración de IPMI)**

Roles de usuario:

- admin (a): **requerido para las modificaciones de propiedades de configuración de especificaciones de IPMI**
- Administrator u Operator: requerido al utilizar el servicio de IPMI (IPMItool) desde la CLI de Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
Session Timeout (Tiempo de espera de sesión) (timeout=)	Disabled (Desactivado)	*Disabled* |*Enabled, minutes=n* La propiedad Session Timeout de la CLI determina la cantidad de minutos que transcurren hasta que se cierran automáticamente las sesiones de la CLI que están inactivas. De forma predeterminada, no hay ningún tiempo de espera de la CLI configurado. Si se utiliza la CLI de Oracle ILOM en una consola compartida, se recomienda a los administradores de la red que configuren el tiempo de espera de las sesiones de la CLI con un valor de 15 minutos o menos. **Interfaz web**: para que los cambios hechos en las propiedades de tiempo de espera de las sesiones de la CLI desde la interfaz web tengan efecto en Oracle ILOM, debe hacer clic en Save (Guardar). **Sintaxis de la CLI para el estado de IPMI**: **set /***SP*|*CMM***/cli timeout=***enabled*|*disabled* **minutes=***value*

TABLA 41 Propiedades de configuración del servicio web de WS-Man

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**services/wsman**
- **Web:** **ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > WS-MAN > WS-Man Settings (Configuración de WS-Man)**
- **Rol de usuario:** **admin (a) (requerido para todas las modificaciones de propiedades)**

Propiedad	Valor predeterminado	Descripción
State (Estado) (`state=`)	Enabled (Activado)	*Enabled* |*Disabled* El estado del servicio web de WS-Man está activado de forma predeterminada. Si es necesario, se puede desactivar el estado del servicio web de WS-Man. **Interfaz web**: para que los cambios hechos en el estado de WS-Man desde la interfaz web tengan efecto en Oracle ILOM, debe hacer clic en Save (Guardar). **Sintaxis de la CLI para el estado de WS-Man**: **set /***SP*|*CMM***/services/wsman state=***enabled***|***disabled* **Información relacionada**: ■
Mode (Modo) (`mode=http`)	HTTP	*HTTP*|*HTTPS* La propiedad Mode está establecida en HTTP de forma predeterminada. Para mejorar la seguridad, se la puede establecer en HTTPS. **Sintaxis de la CLI para el modo de WS-Man**: **set /***SP*|*CMM***/services/wsman mode=***http*|*https*
HTTP Port (Puerto HTTP) (`http_port=`)	8889	*8889* |*user_defined* Cuando la propiedad State está activada y la propiedad Mode está establecida en HTTP, Oracle ILOM utiliza el puerto TCP 8889 para el servicio web de WS-Man. Si es necesario, el valor predeterminado de la propiedad de puerto se puede cambiar. **Sintaxis de la CLI para el puerto HTTP de WS-MAN**: **set /***SP*|*CMM***/services/wsman http_port=***n*

TABLA 41 Propiedades de configuración del servicio web de WS-Man *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/services/wsman
- **Web:** ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > WS-MAN > WS-Man Settings (Configuración de WS-Man)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Propiedad	Valor predeterminado	Descripción
HTTPS Port (Puerto HTTPS) (https_port=)	8888	*8888* |*user_defined* Cuando la propiedad State está activada y la propiedad Mode está establecida en HTTP, Oracle ILOM utiliza el puerto TCP 8888 para el servicio web de WS-Man. Si es necesario, el valor predeterminado de la propiedad de puerto se puede cambiar. **Sintaxis de la CLI para el puerto HTTPS de WS-Man**: **set /SP|CMM/services/wsman https_port=***n*

TABLA 42 Propiedades de configuración de mensajes de rótulo

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /SP|CMM/preferences/banner
- **Web:** ILOM Administration (Administración de ILOM) > Management Access (Acceso de gestión) > Banner Messages (Mensajes de rótulo)
- **Rol de usuario:** admin (a) (requerido para la modificación de propiedades)

Propiedad	Valor predeterminado	Descripción
Connect Message (Mensaje de conexión) (connect_message=)		Complete la propiedad Connect Message con el contenido que desea que aparezca en las interfaces de Oracle ILOM al conectarse a Oracle ILOM. **Sintaxis de la CLI para configurar el mensaje de conexión:** **set /SP/preferences/banner connect_message=**<*content*>
Login Message (Mensaje de inicio de sesión) (login_message=)		Complete la propiedad Login Message con el contenido que desea que aparezca en las interfaces de Oracle ILOM después de iniciar sesión en Oracle ILOM. **Sintaxis de la CLI para configurar el mensaje de inicio de sesión:** **set /SP/preferences/banner login_message=**<*content*>
Login Message Acceptance (Aceptación del mensaje de inicio de sesión) (login_message_acceptance=)	Disabled (Desactivado)	*Disabled* |*Enable*d Configure la propiedad Login Banner Acceptance con el valor Enabled (Activado) para que aparezca el mensaje de rótulo. **Sintaxis de la CLI para la aceptación del mensaje de inicio de sesión**: **set /SP/preferences/banner login_message_acceptance=***disabled*|*enabled*

Modificación de las propiedades predeterminadas de configuración de la conectividad

Los administradores de la red pueden aceptar o modificar las propiedades predeterminadas de conectividad de Oracle ILOM. Para modificar las propiedades predeterminadas de conectividad de Oracle ILOM, consulte las siguientes tablas:

- Tabla 43
- Tabla 44
- Tabla 45

TABLA 43 Propiedades de configuración de conectividad de red

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**network**
- **Web:** ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Requisitos:

- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
State (Estado) (`state=`)	Enabled (Activado)	*Enabled* |*Disabled* La propiedad State de la red está activada de forma predeterminada. Esta propiedad siempre debe estar activada para que Oracle ILOM funcione en entornos de red IPv4 o en entornos de red IPv6 de doble pila. **Sintaxis de la CLI para configurar el estado de la red**: **set /***SP*|*CMM***/network pendingstate=***enabled***|***disabled*
MAC Addres (Dirección MAC) Out of Band MAC Address (Dirección MAC fuera de banda) Sideband MAC Address (Dirección MAC de banda lateral)	Read-only (Sólo lectura)	`macaddress=`| `outofbandaddress=` |`sidebandmacaddress=` Las direcciones MAC (Media Access Control) del SP del servidor y el CMM se configuran en fábrica. Las propiedades MAC Address del SP y el CMM son de sólo lectura en Oracle ILOM, por lo que no se pueden configurar. **Sintaxis de la CLI para mostrar las propiedades de la dirección MAC**: **show /***SP*|*CMM***/network**

TABLA 43 Propiedades de configuración de conectividad de red *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI:** `/`*SP*`|`*CMM*`/network`
- **Web: ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)**
- **Rol de usuario: admin (a) (requerido para todas las modificaciones de propiedades)**

Requisitos:
- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
Management Port (Puerto de gestión) `(managementport=)`	MGMT	*MGMT* |*NETn* Todos los servidores que vienen con Oracle ILOM incluyen un puerto de gestión de red físico (`MGT`) que se utiliza para conectarse con Oracle ILOM por medio de una red. Algunos sistemas que vienen con Oracle ILOM también admiten la gestión de banda lateral. La gestión de banda lateral comparte el uso de un puerto de datos físico (NET*n*) en el servidor para permitir el acceso de la red al sistema operativo host y Oracle ILOM. Para los sistemas que admiten esta opción, los administradores pueden aceptar la propiedad predeterminada Management Port (MGMT) o modificarla para utilizar la gestión de banda lateral (NET*n*). **Sintaxis de la CLI para el puerto de gestión del SP**: **`set /SP/network pendingmanagementport=`***MGMT*|*NETn* **Información relacionada**: ■ "Conexión de gestión de red de banda lateral" en la página 15 ■ "Conexión de gestión de red dedicada (predeterminado)" en la página 12

TABLA 43 Propiedades de configuración de conectividad de red *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**network**
- **Web:** **ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)**
- **Rol de usuario: admin (a) (requerido para todas las modificaciones de propiedades)**

Requisitos:

- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
IPv4 IP Discovery Mode (Modo de detección de direcciones IP IPv4) (`ipdiscovery=`)	DHCP	*DHCP* |*Static* La propiedad para el modo de detección de IPv4 de Oracle ILOM está establecida en DHCP de forma predeterminada. Cuando esta propiedad está establecida en DHCP, Oracle ILOM utiliza DHCP para determinar la dirección de red física del SP del servidor o el CMM. De manera opcional, los administradores de la red pueden desactivar la propiedad DHCP y configurar una dirección de red IPv4 estática, una dirección de máscara de red y una dirección de puerta de enlace para el SP del servidor o el CMM. **Nota**: Cuando DHCP está establecido, Oracle ILOM utiliza la propiedad Auto DNS predeterminada para asignar el servidor de nombres y la ruta de búsqueda del DNS. Para configuraciones de DHCP de doble pila, la propiedad DNS de Oracle ILOM se puede configurar para recibir la información del DNS del servidor DHCP IPv4 o IPv6. **Sintaxis de la CLI para el modo de detección de direcciones IP IPv4**: `set /`*SP*|*CMM*`/network pendingipdiscoverymode=`*dhcp*|*static* **Información relacionada**: ■ Tabla 44
IPv4 DHCP Client ID (ID de cliente DHCP) (`dhcp_clientid=`)	None (Ninguno)	*None*|*SysID* La propiedad DHCP Client ID está establecida en None de forma predeterminada. Si lo desean, los administradores de la red pueden configurar un SysID (identificador de sistema) para el cliente DHCP. **Sintaxis de la CLI para el ID del cliente DHCP de IPv4**: **set /***SP*|*CMM***/network pendingdhcip_clientid=***none*|*sysid* **Información relacionada**: ■ "Asignación de la información sobre identificación del sistema" en la página 121

TABLA 43 Propiedades de configuración de conectividad de red *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**network**
- **Web:** **ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)**
- **Rol de usuario:** **admin (a) (requerido para todas las modificaciones de propiedades)**

Requisitos:

- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
IPv4 Network Address (Dirección de red) Netmask Address (Dirección de máscara de red) Gateway Address (Dirección de puerta de enlace)	Modo de detección de direcciones IP estáticas, desactivado	ipaddress=|ipnetmask=|ipgateway= Las propiedades de IP4 que el usuario puede configurar para la red, la máscara de red y la puerta de enlace están desactivadas de forma predeterminada en Oracle ILOM. Si lo desean, los administradores de la red pueden configurar un valor estático para la propiedad IP Discovery Mode (Modo de detección de direcciones IP) y completar manualmente las direcciones IPv4 estáticas correspondientes a la red, la máscara de red y la puerta de enlace. **Sintaxis de la CLI para las direcciones IPv4 estáticas**: **set /***SP*|*CMM***/network pendingipaddress=***value* **pendingipnetmask=***value* **pendingipgateway=***value* **Información relacionada**: ■ “Formato de entrada para direcciones IPv4 e IPv6” en la página 89
IPv6 State (Estado) (/ipv6/ state=)	Enabled (Activado)	*Enabled* |*Disabled* La propiedad State de IPv6 está activada de forma predeterminada en Oracle ILOM. Si lo desean, los administradores de la red pueden desactivar el estado de la red IPv6 de los entornos de red que no dependan de la traducción de direcciones IP de doble pila. **Nota**: El estado de IPv6 debe estar activado en Oracle ILOM para las traducciones de direcciones IP de doble pila. **Sintaxis de la CLI para el estado de IPv6**: **set /***SP*|*CMM***/network/ipv6 pendingaddress=***enabled*|*disabled*

TABLA 43 Propiedades de configuración de conectividad de red *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**network**
- **Web:** **ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)**
- **Rol de usuario: admin (a) (requerido para todas las modificaciones de propiedades)**

Requisitos:

- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
IPv6 Autoconfig (Configuración automática de IPv6) `(/ipv6 autoconfig=)`	Stateless (Sin estado), Enabled (Activado)	*Stateless* |*None* La propiedad IPv6 Autoconfig está establecida en Stateless de forma predeterminada en Oracle ILOM. Cuando la propiedad Autoconfig Stateless está activada, Oracle ILOM obtiene la dirección IPv6 del SP del servidor o el CMM de un enrutador de red configurado para IPv6. Cuando la propiedad IPv6 Autoconfig Stateless está establecida en None, Oracle ILOM no puede utilizar Autoconfig Stateless para obtener la dirección de red IPv6 del SP del servidor o el CMM. **Consideraciones especiales**: ■ Las opciones de IPv6 Autoconfig Stateless determinan la dirección IP que no tienen ningún tipo de compatibilidad con servidores DHCPv6. ■ El valor de la propiedad de sólo lectura de `dhcpv6_server_duid=` es `none` cuando está activada solamente la propiedad IPv6 Autoconfig Stateless en Oracle ILOM. ■ La propiedad IPv6 Autoconfig Stateless se puede activar simultáneamente en Oracle ILOM cuando DHCPv6_Stateless está activada o cuando DHCPv6_Stateful está activada. **Sintaxis de la CLI para la configuración automática de IPv6**: **set /***SP*|*CMM***/network/ipv6 autoconfig=***stateless*|*none*

TABLA 43 Propiedades de configuración de conectividad de red *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/network
- **Web**: ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)
- **Rol de usuario**: admin (a) (requerido para todas las modificaciones de propiedades)

Requisitos:

- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
DHCPv6 Autoconfig (Configuración automática de DHCPv6) (`/ipv6 autoconfig=`)	None (Ninguno), Disabled (Desactivado)	*DHCPv6_Stateless* |*DHCP_Stateful* |*None* La propiedad DHCPv6 Autoconfig está desactivada (establecida en None) de forma predeterminada en Oracle ILOM. Cuando esta propiedad está establecida en None, Oracle ILOM no puede obtener la dirección de red ni la información de DNS del SP del servidor o el CMM de los servidores DHCPv6 de la red. Si lo desean, los administradores de la red pueden hacer que un servidor DHCPv6 conectado a la red asigne la dirección IPv6 y la información del DNS para el SP o el CMM estableciendo la propiedad DHCPv6 Autoconfig de Oracle ILOM en uno de los siguientes valores: ■ DHCPv6 Stateless (DHCPv6 sin estado): si se activa, Oracle ILOM utiliza la configuración automática sin estado de DHCPv6 para obtener la dirección IPv6 y la información del DNS para el SP del servidor o el CMM. ■ DHCPv6 Stateful (DHCPv6 con estado): si se activa, Oracle ILOM utiliza la configuración automática con estado de DHCPv6 para obtener la dirección IPv6 y la información del DNS para el SP del servidor o el CMM. **Consideraciones especiales**: ■ En Oracle ILOM, la propiedad IPv6 Autoconfig Stateless se puede activar simultáneamente cuando DHCPv6 Autoconfig está activada para usar: DHCPv6_Stateless o DHCPv6_Stateful. ■ Para configuraciones DHCP de doble pila, la propiedad DNS de Oracle ILOM se puede configurar para recibir la información del DNS del servidor DHCP IPv4 o IPv6. ■ El ID exclusivo del servidor DHCPv6 que Oracle ILOM utilizó la última vez para recuperar la información de la red DHCPv6 es identificado por la propiedad dhcpv6_server_duid. **Sintaxis de la CLI para la configuración automática de DHCPv6**: `set /`*SP*|*CMM*`/network/ipv6` `autoconfig=`*dhcpv6_stateless*|*dhcpv6_stateful*|*none*

TABLA 43 Propiedades de configuración de conectividad de red *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** /*SP*|*CMM*/**network**
- **Web:** ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Requisitos:

- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
Link-Local IPv6 Address (Dirección IPv6 local de vínculo) `(/ipv6 link_local_ipaddress=)`	Read-only (Sólo lectura)	La propiedad de sólo lectura Link-Local IPv6 Address es una dirección no enrutable que puede utilizar para conectarse al SP de Oracle ILOM (o al CMM) desde otro nodo activado para IPv6 de la misma red. Oracle ILOM aplica los siguientes principios para generar la dirección local de vínculo para el SP o el CMM: ■ Oracle ILOM utiliza la dirección MAC del SP o el CMM en conjunto con el prefijo del identificador local de vínculo. ■ En el inicio, Oracle ILOM utiliza el protocolo de detección de dirección duplicada (DAD) para asegurarse de que la dirección local de vínculo del SP (o el CMM) sea exclusiva. **Sintaxis de la CLI para la dirección local de vínculo**: **show /***SP*|*CMM***/network/ipv6**
IPv6 Static IP Address (Dirección IP estática) `(/ipv6 static_ipaddress=)`	None (Ninguno)	Cuando el estado de IPv6 está activado, los administradores de la red pueden asignar una dirección IPv6 estática al SP o el CMM. Los parámetros para especificar la dirección IP estática y la máscara de red de IPv6 son: *IPv6_address/subnet_mask_length_in_bits*. La dirección de la puerta de enlace se configura automáticamente. **Ejemplo**: fec0:a:8:b7:214:4fff:feca:5f7e/64 **Sintaxis de la CLI para direcciones IPV6 estáticas**: **set /***SP*|*CMM***/network/ipv6 static_ipaddress=***ipaddress***/***subnetmask*
IPv6 Gateway (Puerta de enlace IPv6) (`/ipv6 ipgateway=`)	Read-only (Sólo lectura)	La dirección de puerta de enlace IPv6 de sólo lectura que se presenta en esta propiedad se obtiene de un enrutador IPv6 de la red. **Sintaxis de la CLI para la puerta de enlace IPv6**: *show /SP/CMM/network/ipv6*

TABLA 43 Propiedades de configuración de conectividad de red *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI**: /*SP*|*CMM*/**network**
- **Web**: **ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)**
- **Rol de usuario**: **admin (a) (requerido para todas las modificaciones de propiedades)**

Requisitos:

- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
Dynamic IPv6 Address (Dirección IPv6 dinámica) (`/ipv6 dynamic_ipaddress_`*n*)	Read-only (Sólo lectura)	Oracle ILOM registra direcciones IPv6 dinámicas cuando sucede lo siguiente: ■ Una o ambas propiedades de `Autoconfig Stateless` y `Autoconf DHCPv6_Stateful` está activadan en Oracle ILOM. ■ El enrutador IPv6 de la red o el servidor DHCPv6 registran varias direcciones de red dinámicas para el SP del servidor o el CMM. **Consideraciones especiales**: ■ Oracle ILOM almacena hasta 10 direcciones dinámicas en una estructura interna. ■ Oracle ILOM responde a todas las direcciones de red dinámicas. ■ Si está configurada solamente la propiedad `Autoconfig DHCPv6_Stateless`, no se registran direcciones de red dinámicas en las interfaces de Oracle ILOM. **Sintaxis de la CLI para direcciones IPV6 dinámicas:** **show /***SP*|*CMM***/network/ipv6**

TABLA 43 Propiedades de configuración de conectividad de red *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI:** /*SP*|*CMM*/**network**
- **Web:** **ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Settings (Configuración de red)**
- **Rol de usuario:** **admin (a) (requerido para todas las modificaciones de propiedades)**

Requisitos:
- Es necesario confirmar las modificaciones de red pendientes en la CLI para que tengan efecto en Oracle ILOM.
- Las modificaciones de red que se hagan desde la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
Botón Save (Guardar) (`commitpending=true`)	Todas las modificaciones de red pendientes	**Interfaz web**: todas las modificaciones hechas en la página Network Settings (Configuración de red) se deben guardar para que tengan efecto en Oracle ILOM. **CLI**: todas las modificaciones de la red que estén pendientes se deben confirmar en el destino `/network`. **Consideraciones especiales**: ■ Las modificaciones de IPv4 que estén pendientes entran en efecto después de haberlas confirmado o guardado. ■ La asignación de una nueva dirección IPv4 estática a un dispositivo gestionado pondrá fin a todas las sesiones activas de Oracle ILOM con el SP o el CMM. Para volver a iniciar sesión en Oracle ILOM, abra una nueva sesión del explorador y escriba la dirección IPv4 recientemente asignada. ■ Las modificaciones de IPv6 que están pendientes entran en efecto después de haberlas confirmado o guardado. No es necesario confirmar los cambios hechos en las propiedades de configuración automática desde la CLI. ■ Las direcciones IPv6 de configuración automática recién adquiridas no afectarán ninguna de las sesiones de Oracle ILOM actualmente conectadas con el dispositivo gestionado (SP o CMM). **Sintaxis de la CLI para confirmar las modificaciones de IPv4 pendientes**: **set /***SP*|*CMM***/network pendingstate=***enabled*|*disabled* **pendingipdiscovery=***static*|*dhcp* **pendingipaddress=***value* **pendingipgateway=***value* **pendingipnetmask=***value* **commitpending=true** **Sintaxis de la CLI para confirmar las modificaciones de IPv6 pendientes:** **set /***SP*|*CMM***/network pendingstate=***enabled*|*disabled* **pending_static_ipaddress=***ip6_address***/** *subnet_mask_length_in_bits* **commitpending=true** **Información relacionada**: ■ "Prueba de la conectividad de IPv4 e IPv6" en la página 128

TABLA 44 Propiedades de configuración del DNS

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI**: `/SP|CMM/clients/dns`
- **Web**: **ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > DNS > DNS Configuration (Configuración de DNS)**
- **Rol de usuario**: **admin (a) (requerido para la modificación de propiedades)**

Propiedad	Valor predeterminado	Descripción
Auto DNS via DHCP (DNS automático por medio de DHCP) (`auto_dns=`)	Enabled (Activado)	Enabled |Disabled La propiedad Auto DNS via DHCP está activada de forma predeterminada en Oracle ILOM. Cuando esta propiedad está activada, Oracle ILOM recupera automáticamente la información del DNS del servidor DHCP. Si lo desean, los administradores de la red pueden desactivar la propiedad Auto DNS para configurar la información del DNS manualmente en Oracle ILOM. **Sintaxis de la CLI para el DNS automático por medio de DHCP:** `set /`*SP*|*CMM*`/clients/dns auto_dns=`*enabled*|*disabled*
DNS Named Server (Servidor de nombres del DNS) (`nameserver=`)	None (Ninguno)	Cuando la propiedad Auto DNS está desactivada, se pueden configurar manualmente hasta tres direcciones IP en la propiedad DNS Named Server. Cuando escriba varias direcciones IP, siga estas directrices: ■ Las direcciones se deben separar con una coma. ■ Si se utilizan direcciones IPv4 e IPv6, escriba primero las direcciones IPv4. **Sintaxis de la CLI para el servidor de nombres del DNS**: **`set /`***SP*|*CMM***`/clients/dns nameserver=`***ip_address_1, ipaddress_2, ipaddress_3*
DNS Search Path (Ruta de búsqueda de DNS) (`searchpath=`)	None (Ninguno)	Cuando la propiedad Auto DNS está desactivada, se pueden configurar manualmente hasta seis sufijos de dominio en la propiedad DNS Search Path. Los sufijos de búsqueda se deben separar con una coma. **Sintaxis de la CLI para la ruta de búsqueda del DNS:** **`set /SP|CMM/clients/dns searchpath=`** *domain_1.com, domain_2.edu, and so on ...*

TABLA 44 Propiedades de configuración del DNS *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** `/SP|CMM/clients/dns`
- **Web:** ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > DNS > DNS Configuration (Configuración de DNS)
- **Rol de usuario:** admin (a) (requerido para la modificación de propiedades)

Propiedad	Valor predeterminado	Descripción
DNS Timeout (Tiempo de espera de DNS) (`timeout=`)	5 seconds (5 segundos)	Entero entre 1 y 10 El valor de la propiedad DNS Timeout especifica la cantidad de segundos que tiene el servidor DNS para completar cada consulta del DNS. Si lo desean, los administradores de la red pueden aumentar o reducir el valor predeterminado de tiempo de espera asignado al servidor DNS. **Sintaxis de la CLI para el tiempo de espera del DNS**: **`set /SP|CMM/clients/dns timeout=`***n* **Tema relacionado**: ■ "Configuración de ejemplo de DNS dinámico" en la página 119
DNS Retries (Reintentos de DNS) (`retries=`)	1 retry (1 reintento)	Entero entre 0 y 4 El valor de la propiedad DNS Retries especifica la cantidad de veces que se reintenta cada consulta del DNS si se agota el tiempo de espera. Si lo desean, los administradores de la red pueden aumentar o reducir el valor predeterminado de la propiedad DNS Retries. **Sintaxis de la CLI para los reintentos del DNS**: `set /`*SP*|*CMM*`/clients/dns retries=`*n*
Botón Save (Guardar) (sólo web)		**Interfaz web**: todos los cambios hechos en la página DNS Configuration (Configuración de DNS) se deben guardar en Oracle ILOM para que tengan efecto.

TABLA 45 Propiedades de configuración de los puertos serie

Destino configurable de la interfaz de usuario:

- **CLI:** `/SP/serial/portsharing`
- **Web:** ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Serial Port (Puerto serie) > Serial Port Settings (Configuración de puerto serie)
- **Rol de usuario:** Admin (a) (requerido para la modificación de propiedades)

Propiedad	Valor predeterminado	Descripción
Owner (Propietario) (`owner =`)	SP	*SP* |*hostserver* La propiedad Owner del puerto serie se puede configurar en algunos servidores de Oracle. Para obtener información adicional, consulte "Propietario del puerto de gestión serie" en la página 89. **Sintaxis de la CLI para el propietario del puerto serie**: **`set /SP/serial/portsharing owner=`***SP*|*hostserver*
Host Serial Port (Puerto serie de host) (`/host pendingspeed= flowcontrol=`)	Velocidad en baudios = 9600 Control de flujo = ninguno	`Baud Rate =` *9600* |`Flow Control =` *Software* |*Hardware*|*None* La propiedad Host Serial Port se puede configurar en algunos servidores de Oracle. Los valores de la opción Host Serial Port deben coincidir con los valores de la propiedad configurados para el puerto de la consola serie en el servidor host. Con frecuencia se lo denomina puerto serie 0, COM1 o /dev/ttyS0. **Sintaxis de la CLI para el puerto serie del host**: **`set /`***SP*|*CMM***`/serial/host pendingspeed=`***value* **`flowcontrol=`***value* **`commitpending=true`**
External Serial Port (Puerto serie externo) (`/external pendingspeed= flowcontrol=`)	Velocidad en baudios = 9600 Control de flujo = ninguno	`Baud Rate =` *9600* |`Flow Control =` *None* El puerto serie externo de un dispositivo gestionado es el puerto de gestión serie (SER MGT). Si lo desean, los administradores de la red pueden cambiar la velocidad en baudios predeterminada para el puerto serie externo. **Sintaxis de la CLI para el puerto serie externo**: **`set /`***SP*|*CMM***`/serial/external pendingspeed=`***value* **`commitpending=true`**
Botón Save (Guardar) (sólo web)		**Interfaz web**: todos los cambios hechos en la página Serial Port Settings (Configuración de puerto serie) se deben guardar en Oracle ILOM para que tengan efecto.

Configuración de ejemplo de DNS dinámico

Mediante la configuración de un servicio de nombres de dominio dinámico (DDNS), puede aprovechar DHCP aún más para que el servidor DNS de su entorno de red reconozca automáticamente los nombres de host de todos los sistemas de Oracle ILOM agregados mediante DHCP.

Cuando el servicio DDNS está configurado, los administradores de la red pueden determinar el nombre de host de un SP o un CMM de Oracle ILOM específico combinando el número serie del producto con uno de estos prefijos: SUNSP o SUNCMMn. Por ejemplo, si el número de serie de un producto es 0641AMA007, el nombre del host para un SP del servidor sería SUNSP-0641AMA007, el nombre del host para un CMM instalado en el chasis sería SUNCMM-0641AMA007 y los nombres de host de dos CMM instalados en el chasis serían SUNCMM0-0641AMA007 y SUNCMM1-0641AMA007.

▼ Ejemplo: Configuración de DDNS

En este ejemplo, se describe la configuración típica del DDNS.

Suposiciones:

Para este ejemplo de configuración de DDNS, se hacen las siguientes suposiciones:

- Existe un único servidor que controla tanto DNS como DHCP en la red en la que reside el SP.
- La dirección de red del SP es 192.168.1.0.
- La dirección del servidor DHCP/DNS es 192.168.1.2.
- Las direcciones IP de 192.168.1.100 a 192.168.1.199 se utilizan como conjunto para proporcionar direcciones al SP y a otros clientes.
- El nombre del dominio es `example.com`.
- No se ha realizado ninguna configuración de DNS ni DHCP. Si se hubiese realizado, utilice los archivos `.conf` de este ejemplo como guía para actualizar la configuración existente.

Nota – La forma en la que configure DDNS dependerá de la infraestructura que utilice en su sitio. Los sistemas operativos Oracle Solaris, Linux y Microsoft Windows admiten soluciones de servidor que ofrecen la funcionalidad de DDNS. En este ejemplo de configuración, se utiliza Debian r4.0 como entorno de sistema operativo del servidor.

Puede utilizar los siguientes pasos y los archivos modelo que se proporcionan aquí, con modificaciones específicas según el sitio, para realizar su propia configuración de DDNS.

1 **Instale los paquetes `bind9` y `dhcp3-server` de la distribución de Debian.**

La instalación del paquete `dnsutils` brinda acceso a `dig`, `nslookup` y otras herramientas útiles.

2 **Con `dnssec-keygen`, genere una clave compartida para que los servidores DHCP y DNS controlen el acceso a los datos del DNS.**

3 **Cree un archivo de configuración del DNS con el nombre `/etc/bind/named.conf` que contenga lo siguiente:**

```
options {
  directory "/var/cache/bind";
  auth-nxdomain no;    # conform to RFC1035
  listen-on-v6 { any; };
};
// prime the server with knowledge of the root servers
zone "." {
  type hint;
  file "/etc/bind/db.root";
};
// be authoritative for the localhost forward and reverse zones, // and for broadcast zones as per RFC 1912
zone "localhost" {
  type master;
  file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
  type master;
  file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
  type master;
  file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
  type master;
  file "/etc/bind/db.255";
};
// additions to named.conf to support DDNS updates from dhcp server
key server.example.com {
  algorithm HMAC-MD5;
  secret "your-key-from-step-2-here"
};
zone "example.com" {
  type master;
  file "/etc/bind/db.example.com";
  allow-update { key server.example.com; };
};
zone "1.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/db.example.rev";
  allow-update { key server.example.com; };
};
```

4 **Agregue archivos de zona vacíos para la red local.**

Los archivos de zona vacíos se deben denominar `/etc/bind/db.example.com` y `/etc/bind/db.example.rev`.

Si copia los archivos de distribución `db.empty` suministrados, será suficiente; se actualizarán automáticamente mediante el servidor DNS.

5 Cree un archivo `/etc/dhcp3/dhcpd.conf` que contenga lo siguiente:

```
ddns-update-style interim;
ddns-updates      on;
server-identifier server;
ddns-domainname   "example.com.";
ignore client-updates;
key server.example.com {
  algorithm hmac-md5;
  secret your-key-from-step-2-here;
}
zone example.com. {
  primary 127.0.0.1;
  key server.example.com;
}
zone 1.168.192.in-addr.arpa. {
  primary 127.0.0.1;
  key server.example.com;
}
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.199;
  option domain-name-servers 192.168.1.2;
}
```

6 Después de realizar los pasos del 1 al 5, ejecute la secuencia de comandos `/etc/init.d` para iniciar los servidores DNS y DHCP.

Una vez que se ejecuten los servidores, podrá acceder automáticamente a los nuevos SP de Oracle ILOM configurados para DHCP utilizando su nombre de host cuando estén encendidos. Use los archivos de registro, `dig`, `nslookup` y otras utilidades para depurar, si es necesario.

Más información Referencias

Para obtener más información sobre los servidores DHCP y DNS de Linux que se utilizan en este ejemplo, consulte el sitio web de Internet Systems Consortium: http://www.isc.org/ http://www.isc.org/

Asignación de la información sobre identificación del sistema

Oracle ILOM proporciona un conjunto de propiedades configurables para ayudar a identificar un dispositivo gestionado específico en el entorno. Los administradores del sistema pueden utilizar estos parámetros para identificar de manera exclusiva la ubicación física de un dispositivo gestionado, el punto de contacto de un dispositivo gestionado y el nombre de host asignado a un dispositivo gestionado. Si desea leer información más detallada sobre la configuración de identificación del sistema, vea la siguiente tabla.

TABLA 46 Propiedades de configuración de identificación de dispositivos

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** `/SP/`
- **Web:** ILOM Administration (Administración de ILOM) > Identification (Identificación)
- **Rol de usuario:** Admin (a) (requerido para la modificación de propiedades)

Propiedad	Valor predeterminado	Descripción
Host Name (Nombre de host) `(hostname=)`	None (Ninguno)	La propiedad Host Name, cuando se la define, ayuda a identificar un dispositivo gestionado que está conectado a una red de equipos. El valor de la propiedad Host Name puede contener hasta 60 caracteres. Debe comenzar por una letra y contener solamente caracteres alfanuméricos, guiones o caracteres de subrayado. **Sintaxis de la CLI para el nombre del host**: **set /***SP*|*CMM* **hostname=***value*
System Identifier (Identificador del sistema) `(/system_identifier=)`	None (Ninguno)	La propiedad System Identifier, si se la define, ayuda a identificar el dispositivo gestionado en el elemento de carga útil de una captura de SNMP. El valor de la propiedad System Identifier puede contener hasta 60 caracteres en cualquier combinación de teclas de un teclado estándar, excepto las comillas. Esta propiedad se puede configurar en el SP del servidor y el CMM. **Sintaxis de la CLI para el identificador del sistema**: set /*SP*|*CMM* system_identifier=*value*
System Contact (Contacto del sistema) `(/system_contact=)`	None (Ninguno)	La propiedad System Contact, si se la define, ayuda a identificar el punto de contacto para el dispositivo gestionado, por ejemplo, el nombre o la dirección de correo electrónico de la persona que está a cargo del dispositivo. El valor de la propiedad System Contact puede estar compuesto por una cadena de texto formada por cualquier combinación de teclas de un teclado estándar, excepto las comillas. **Sintaxis de la CLI para el contacto del sistema**: set /SP|CMM system_contact=*value*
System Location (Ubicación del sistema) `(/system_location=)`	None (Ninguno)	La propiedad System Location, si se la define, ayuda a identificar la ubicación física de un dispositivo gestionado, por ejemplo, la ubicación de un identificador de bastidor o un centro de datos. El valor de la propiedad System Location puede estar compuesto por una cadena de texto formada por cualquier combinación de teclas de un teclado estándar, excepto las comillas. **Sintaxis de la CLI para la ubicación del sistema**: **set /***SP*|*CMM* **system_location=***value*

TABLA 46 Propiedades de configuración de identificación de dispositivos *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI**: `/SP/`
- **Web**: ILOM Administration (Administración de ILOM) > Identification (Identificación)
- **Rol de usuario**: Admin (a) (requerido para la modificación de propiedades)

Propiedad	Valor predeterminado	Descripción
Physical Presence Check (Control de presencia física) (`/check_physical_presence=`)	Enabled (Activado)	La propiedad Physical Presence Check afecta el comportamiento para la recuperación de la contraseña de la cuenta `root` preconfigurada de Oracle ILOM. ■ Enabled (true) (Activado [verdadero]): si la propiedad está activada, se debe pulsar el botón Locator (Localizador) del sistema físico para poder recuperar la contraseña predeterminada de Oracle ILOM. ■ Disabled (false) (Desactivado [falso]): si la propiedad está desactivada, se puede restablecer la contraseña de administrador predeterminada de Oracle ILOM sin pulsar el botón Locator (Localizador) del sistema físico. **Sintaxis de la CLI para el control de presencia física**: `set /SP|CMM check_physical_presence=`*true*|*false* **Tema relacionado**: ■ Tabla 12
Botón Save (Guardar) (sólo web)		**Interfaz web**: todos los cambios hechos en la página Identification (Identificación) se deben guardar en Oracle ILOM para que tengan efecto.

Configuración de propiedades para el reloj del SP o el CMM

Con la implementación inicial de Oracle ILOM, los administradores del sistema deben configurar los parámetros del reloj en Oracle ILOM para garantizar que los eventos de gestión del sistema registrados por Oracle ILOM aparezcan con indicadores de fecha y hora correctos.

Los administradores del sistema pueden sincronizar el reloj de Oracle ILOM con un servidor NTP o pueden configurar manualmente la fecha y la hora de manera local en Oracle ILOM con la zona horaria UTC/GMT del servidor host.

Para las propiedades de configuración del reloj de Oracle ILOM, vea la siguiente tabla.

TABLA 47 Propiedades de configuración del reloj de Oracle ILOM

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** `/SP|CMM/clock`
- **Web:** ILOM Administration (Administración de ILOM) > Date and Time (Fecha y hora) > Clock Settings (Configuración de reloj) | Timezones (Zonas horarias)
- **Rol de usuario:** admin (`a`) (requerido para la modificación de propiedades)

Propiedad	Valor predeterminado	Descripción
Date and Time (Fecha y hora) (`datetime=`)	None (Ninguno)	Complete la propiedad Date con el mes, el día y el año. Complete la propiedad Time con las horas y los minutos. **Sintaxis de la CLI para la fecha y la hora**: **set /***SP*|*CMM***/clock datetime=***MMDDhhmmYYYY*
Timezones (Zonas horarias) (`timezones=`)	None (Ninguno)	Abreviaciones de las zonas horarias (PST, EST, etc.) Complete la propiedad Timezones con la zona horaria adecuada. **Sintaxis de la CLI para las zonas horarias**: **set /***SP*|*CMM***/clock timezones=***3_to_4_characters*
Synchronize Time with NTP Server (Sincronizar hora con servidor NTP) (`usentpserver=`)	Disabled (Desactivado)	*Enabled*|*Disabled* Active esta propiedad para indicar a Oracle ILOM que sincronice la configuración del reloj con el servicio NTP de la red. **Nota –** Se necesita la configuración mínima de una dirección IP de un servidor NTP. Vea la propiedad NTP Server. **Sintaxis de la CLI para sincronizar la hora con el servidor NTP**: **set /***SP*|*CMM***/clock usentpserver=***enabled*|*disabled*
NTP Server (Servidor NTP) 1 (2) (`/SP/clients/ntp/server`*n*`=`)	None (Ninguno)	Complete las propiedades Server 1 (Servidor 1) o Server 2 (Servidor 2) con la dirección IP de un servidor NTP. **Sintaxis de la CLI para configurar la dirección IP del servidor NTP**: **set /SP/clients/ntp/server1=***ip_address*
Botón Save (Guardar) (sólo web)		**Interfaz web**: todos los cambios hechos en la página Clock Settings (Configuración de reloj) y la página Timezone Settings (Configuración de zona horaria) se deben guardar en Oracle ILOM para que tengan efecto.

Consulte la documentación del servidor de Oracle para determinar lo siguiente:

- Durante el reinicio del SP se puede mantener la hora indicada por Oracle ILOM.
- Si la hora actual en Oracle ILOM se puede sincronizar con el host en el momento de iniciarlo.
- El sistema es compatible con un elemento de reloj en tiempo real que almacena el tiempo.

Resoluciones sugeridas para problemas de conectividad de red

Resolución de configuraciones de seguridad de explorador web

A partir de Oracle ILOM 3.1.0, los usuarios de Internet Explorer (IE) 6 ya no se pueden conectar con la interfaz web sin antes realizar una de dos tareas:

- **Tarea 1**: actualizar el explorador a IE 7 o posterior u otro explorador que sea equivalente o más reciente.

  O bien:
- **Tarea 2**: modificar las propiedades del servidor web de Oracle ILOM y el certificado y la clave de SSL. Para obtener instrucciones, consulte el siguiente procedimiento:

▼ Modificación de las propiedades predeterminadas de servidor web para admitir Internet Explorer 6

El certificado autofirmado preconfigurado del servidor web que se proporciona con Oracle ILOM utiliza un cifrado más potente que IE 6 no admite.

Para los usuarios que no deseen actualizar de IE 6 a IE 7, se deben modificar las propiedades del servidor web como se indica en el siguiente procedimiento para permitir conexiones de IE 6 con la interfaz web de Oracle ILOM.

Antes de empezar

- Se necesita el rol Admin (a) para modificar las propiedades del servidor web en Oracle ILOM.

1 Inicie sesión en la CLI de Oracle ILOM.

2 Para activar los codificadores débiles, escriba:

```
set /SP|CMM/services/https weak_ciphers=enabled
```

3 Para cargar una clave personalizada, escriba:

```
set /SP|CMM/services/https/ssl/custom_key load_uri=<uri_string >
```

4 Para cargar un certificado personalizado, escriba:

set /*SP*|*CMM***/services/https/ssl/custom_cert load_uri=**<*uri_string*>

Más información Información relacionada:

- Tabla 35

Resolución de problemas de conectividad

Si tiene dificultades para establecer una conexión de red con las interfaces de Oracle ILOM, consulte resoluciones posibles en la siguiente información de IPv4 e IPv6.

- Tabla 48
- Tabla 49

TABLA 48 Solución de problemas de conectividad de IPv4

Problema	Posible solución
No se puede acceder a Oracle ILOM mediante IPv4 desde un cliente de red.	Asegúrese de que la configuración de State (Estado) esté activada en la página Network Settings (Configuración de red) de la interfaz web de Oracle ILOM o en el destino `/SP/network` en la CLI de Oracle ILOM. Otras sugerencias para diagnosticar problemas de red de IPv4: ■ Compruebe que haya una conexión LAN con el puerto físico de gestión (NET MGT). ■ Compruebe que esté activado el servicio de red apropiado en Oracle ILOM: SSH, HTTP o HTTPS. En la interfaz web, haga clic en ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) para comprobar y modificar la configuración de la conectividad de red. ■ Use una herramienta de diagnóstico de red estándar, por ejemplo IPv4 Ping o Traceroute, para probar la conexión de red del dispositivo gestionado. Ejecute `ping` desde la interfaz web o la CLI. O bien, ejecute `traceroute` desde el shell restringido de servicios de Oracle ILOM.
No se puede acceder a la interfaz web de Oracle ILOM con el explorador web Internet Explorer 6 (IE 6).	Los usuarios de Internet Explorer 6 deben actualizar el explorador o cargar certificados personalizados y una clave privada para utilizar SSL en la interfaz web de Oracle ILOM. Si desea obtener instrucciones para cargar un certificado SSL personalizado, consulte Tabla 36.

TABLA 49 Solución de problemas de conectividad de IPv6

Problema	Posible solución
No se puede acceder a la interfaz web de Oracle ILOM mediante una dirección de IPv6.	Asegúrese de que la dirección IPv6 de la dirección URL está entre corchetes, por ejemplo: `https://[2001:db8:0:0:0:0:0:0]`

TABLA 49 Solución de problemas de conectividad de IPv6 *(Continuación)*

Problema	Posible solución
No se puede descargar un archivo mediante una dirección de IPv6.	Asegúrese de que la dirección IPv6 de la dirección URL está entre corchetes, por ejemplo: `load -source tftp://[2001:db8:0:0:0:0:0:0]/desktop.pkg`
No se puede acceder a Oracle ILOM mediante IPv6 desde un cliente de red.	Si se trata de una subred independiente, pruebe lo siguiente: ■ Verifique que Oracle ILOM tiene una dirección dinámica o estática (no sólo una dirección vínculo-local). ■ Compruebe que el cliente de red tenga una dirección IPv6 configurada (no sólo una dirección vínculo-local). Si se trata de la misma subred o una subred independiente, pruebe lo siguiente: ■ Asegúrese de que la propiedad IPv6 State (Estado de IPv6) esté activada en la página Network Settings (Configuración de red) de la interfaz web de Oracle ILOM o en el destino `/SP/network/ipv6` en la CLI de Oracle ILOM. ■ Compruebe que esté activado el servicio de red apropiado en Oracle ILOM: SSH, HTTP o HTTPS. En la interfaz web, haga clic en ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) para comprobar y modificar la configuración de la conectividad de red. ■ Use una herramienta de diagnóstico de red estándar, por ejemplo IPv6 Ping o Traceroute, para probar la conexión de red del dispositivo gestionado. Ejecute `ping6` desde la interfaz web o la CLI. O bien, ejecute `traceroute` desde el shell restringido de servicios de Oracle ILOM.
No se puede acceder a la interfaz web de Oracle ILOM con el explorador web Internet Explorer 6 (IE 6).	Los usuarios de Internet Explorer 6 deben actualizar el explorador o cargar certificados personalizados y una clave privada para utilizar SSL en la interfaz web de Oracle ILOM. Si desea obtener instrucciones para cargar un certificado SSL personalizado, consulte Tabla 36.

Práctica recomendada para configuraciones de árbol de expansión

Dado que el puerto de gestión de red del SP no está diseñado para comportarse como un puerto de conmutador, el puerto de gestión de red del SP no es compatible con funciones de los puertos de conmutador, como el parámetro portfast de árboles de expansión.

Al configurar parámetros de árbol de expansión, tenga en cuenta estas recomendaciones:

- El puerto que se utiliza para conectar el puerto de gestión de red del SP al conmutador de red adyacente siempre debe tratar al puerto de gestión de red del SP como puerto host.

- La opción de árbol de expansión del puerto que se conecta al conmutador de red adyacente debe estar desactivada por completo o configurada de forma mínima con los siguientes parámetros:

Parámetro de árbol de expansión	Configuración recomendada
`portfast`	Active esta interfaz para desplazarse inmediatamente a un estado de reenvío.
`bpdufilter`	No envíe ni reciba BPDU en esta interfaz.
`bpduguard`	No acepte BPDU en esta interfaz.
`cdp`	No active el protocolo de detección en esta interfaz.

▼ Prueba de la conectividad de IPv4 e IPv6

Para enviar una prueba de red desde la dirección de IP y la dirección de la puerta de enlace configuradas en Oracle ILOM a un dispositivo de la red, haga lo siguiente:

● **Elija una de estas posibilidades:**

- **CLI:**

  Para emitir una prueba de conectividad ping desde la CLI, escriba una de las siguientes opciones:

  set /*SP*|*CMM***/network/test ping=***device_ipv4_address_on network*

  set /*SP*|*CMM***/network/test ping6=***device_ipv6_address_on network*

  Si la prueba falla, aparece un mensaje de error. En algunos servidores de Oracle, si la prueba se realiza con éxito, aparece un mensaje de éxito.

- **Web:**

  Para emitir una prueba de conectividad ping desde la interfaz web, haga lo siguiente:

  a. **Haga clic en ILOM Administration (Administración de ILOM) > Connectivity (Conectividad) > Network (Red) > Network Tools (Herramientas de red).**

  b. **En el cuadro de diálogo de las herramientas, seleccione el tipo de prueba, especifique la dirección IP de un dispositivo de la red y, a continuación, haga clic en Test (Probar).**

Más información Información relacionada:

- Tabla 43

Uso de consolas de KVMS remoto para la redirección de servidores host

Descripción	Vínculos
Consulte estas secciones para configurar y utilizar Oracle ILOM Remote Console basada en la GUI para la redirección de KVMS del servidor host.	■ "Configuración inicial para Oracle ILOM Remote Console" en la página 129 ■ "Inicio y uso de Oracle ILOM Remote Console " en la página 137
Consulte estas secciones para configurar y utilizar la consola de Oracle ILOM Storage Redirection de la línea de comandos para la redirección de almacenamiento del host.	■ "Configuración inicial para Oracle ILOM Storage Redirection CLI " en la página 142 ■ "Inicio y uso de Oracle ILOM Storage Redirection CLI" en la página 149
Consulte esta sección si desea obtener instrucciones para iniciar una sesión de redirección serie para el sistema operativo del servidor host.	■ "Inicio y detención de una sesión de redirección serie del host" en la página 157

Información relacionada

- *Guía de seguridad de Oracle ILOM 3.1*, Uso de KVMS remoto de forma segura

Configuración inicial para Oracle ILOM Remote Console

Para configurar Oracle ILOM Remote Console antes del primer uso, consulte estos temas:

- "Requisitos para usar Oracle ILOM Remote Console" en la página 130
- "Configuración de valores de KVMS del cliente local" en la página 131
- "Registro del complemento JDK de 32 bits de Java para el explorador web IE de Windows" en la página 133
- "Registro del complemento JDK de 32 bits de Java para el explorador web Mozilla Firefox" en la página 133
- "Configuración opcional de un modo de bloqueo para proteger el escritorio del servidor host " en la página 134

Requisitos para usar Oracle ILOM Remote Console

Se deben cumplir los siguientes requisitos antes de utilizar Oracle ILOM Remote Console por primera vez.

TABLA 50 Requisitos para usar Oracle ILOM Remote Console

Requisito de configuración	Descripción
Configuración de KVMS	Configure las propiedades del cliente local del SP para el comportamiento de redirección de teclado, video y mouse. **Valores predeterminados**: Estado: activado; modo del mouse: absoluto; calidad de visualización: YUV420; modo de bloqueo: desactivado **Información relacionada**: ■ "Configuración de valores de KVMS del cliente local" en la página 131
Java Runtime Environment	Java Runtime Environment (1.5 o posterior) debe estar instalado en el sistema del cliente local. Para descargar la versión más reciente de Java Runtime Environment, vaya a: `http://java.com`.
JDK y explorador web requeridos	Para redes IPv4, se necesita JDK de 32 bits. Para redes IPv6, se necesita JDK170b36 o superior. Para conocer los exploradores web admitidos, consulte "Exploradores web de sistemas operativos compatibles" en la página 35.
Registro de JDK de 32 bits para redirección de video	El complemento JDK de 32 bits de Java se debe registrar con el explorador web del cliente local antes de utilizar Oracle ILOM Remote Console para redirección de video. **Información relacionada**: ■ "Registro del complemento JDK de 32 bits de Java para el explorador web IE de Windows" en la página 133 ■ "Registro del complemento JDK de 32 bits de Java para el explorador web Mozilla Firefox" en la página 133
Roles de usuario y credenciales de usuario del servidor host	Se necesita el rol Admin (Administrador) (a) en Oracle ILOM para modificar el estado de servicio de KVMS. Se necesita el rol Console (Consola) (c) en Oracle ILOM para modificar las propiedades de KVMS (excluida la propiedad de estado del servicio) e iniciar Oracle ILOM Remote Console. Se necesitan credenciales de usuario del servidor host para obtener acceso al servidor host redirigido.

TABLA 50 Requisitos para usar Oracle ILOM Remote Console *(Continuación)*

Requisito de configuración	Descripción
Uso de redirección serie y redirección de video	Al iniciar Oracle ILOM Remote Console, los usuarios pueden iniciar la sesión de KVMS remoto mediante alguno de los siguientes métodos de redirección: ■ **Serial Redirection (SPARC only) (Redirección en serie [sólo SPARC])**: esta opción está disponible sólo para los SP de servidores SPARC. Si está activada, Oracle ILOM presenta una consola basada en texto para las redirecciones de servidores host serie. ■ **Video Redirection (Redirección de video)**: esta opción está disponible para los CMM, los SP de servidores x86 y los SP de servidores SPARC. Esta opción presenta una consola basada en GUI para el servidor host con video redirigido.
Puertos de comunicación TCP/IP requeridos	De manera predeterminada, Oracle ILOM Remote Console utiliza los siguientes puertos de comunicación TCP/IP: ■ Puerto: 5120 para redirección de CD. ■ Puerto: 5123 para redirección de disquete. ■ Puerto: 5556 para redirección de autenticación de usuarios. ■ Puerto: 7578 para redirección de video. ■ Puerto: 7579 para redirección de servidores SPARC solamente. Si desea obtener una lista completa de los puertos de red que utiliza Oracle ILOM, consulte Tabla 34.

▼ Configuración de valores de KVMS del cliente local

1 Para obtener acceso a los valores de KVMS del SP del servidor en Oracle ILOM, haga lo siguiente:

- **Web: haga clic en Remote Console (Consola remota) > KVMS > KVMS Settings (Configuración de KVMS).**
- **CLI: escriba:**

```
show /SP/services/kvms
```

2 Modifique las siguientes propiedades de KVMS según sea necesario:

Propiedad	Descripción
State (Estado) (servicestate=)	De manera predeterminada, está activada la redirección del estado del servicio de KVMS. Esta propiedad debe estar activada para poder utilizar Oracle ILOM Remote Console. Si se desactiva, también se desactiva el uso de Oracle ILOM Remote Console. **Sintaxis de la CLI para el estado del servicio de KVMS**: **set /SP/services/kvms servicestate=***enabled*|*disabled*
Mouse (mousemode=)	Configure la opción adecuada para el modo del mouse: ■ Relative (default) (Relativo [valor predeterminado]): utilice esta configuración de modo de mouse local si el host remoto ejecuta el sistema operativo Linux. ■ Absolute (Absoluto): utilice esta configuración de modo de mouse local si el host remoto ejecuta el sistema operativo Windows o Solaris. **Sintaxis de la CLI para el modo de mouse de KVMS**: **set /SP/services/kvms mousemode=***absolute*|*relative*
Display Quality (Calidad de visualización) (display_quality=)	Seleccione la opción adecuada de calidad de video: ■ YUV420 (valor predeterminado de fábrica inicial): seleccione esta opción para transmitir un esquema de datos de imagen en color de mayor compresión para obtener una velocidad de transferencia de datos optimizada. ■ YUV444: seleccione esta opción para transmitir un esquema de datos de imagen en color de menor compresión para obtener una mayor resolución de imagen. ■ VQ2: seleccione esta opción para transmitir un esquema de datos de video de menor compresión que funcione mejor para salidas de pantallas de terminales de dos colores. ■ VQ4: seleccione esta opción para transmitir un esquema de datos de video de menor compresión que funcione mejor para salidas de pantallas de terminales de cuatro colores. **Nota –** El valor configurado para la propiedad Display Quality se mantiene aunque se reinicie el SP. Por lo tanto, el valor predeterminado de fábrica inicial (YUV420) no se conserva si se hacen modificaciones. **Sintaxis de la CLI para la calidad de visualización de KVMS:** set /SP/services/kvms display_quality=*YUV420*| *YUV444*|*VQ2*|*VQ4*

Propiedad	Descripción
Host Lock Settings (Configuración de bloqueo de host) (lock_mode=)	Si desea obtener una descripción de las propiedades de bloqueo del host, consulte "Configuración opcional de un modo de bloqueo para proteger el escritorio del servidor host" en la página 134.

3 **Para aplicar las modificaciones, haga clic en Save (Guardar) en la página KVMS Settings (Configuración de KVMS).**

▼ Registro del complemento JDK de 32 bits de Java para el explorador web IE de Windows

1 **En el cliente de Windows, abra el Explorador de Windows (no Internet Explorer).**

2 **En el cuadro de diálogo Explorador de Windows, seleccione Herramientas > Opciones de carpeta y luego seleccione la ficha Tipos de archivo.**

3 **En la ficha Tipos de archivo, realice las siguientes acciones:**

a. **En la lista de tipos de archivo registrados, seleccione el tipo de archivo JNLP y haga clic en Cambiar.**

b. **En el cuadro de diálogo Abrir con, haga clic en Examinar para seleccionar el archivo JDK de 32 bits.**

c. **Haga clic en la casilla de verificación Usar siempre el programa seleccionado para abrir este tipo de archivos.**

d. **Haga clic en Aceptar y, a continuación, inicie Oracle ILOM Remote Console.**

Para obtener instrucciones, consulte "Inicio y uso de Oracle ILOM Remote Console" en la página 137.

▼ Registro del complemento JDK de 32 bits de Java para el explorador web Mozilla Firefox

1 **Inicie Oracle ILOM Remote Console desde la interfaz web de Oracle ILOM.**

Haga clic en Remote Console (Consola remota) > Redirection (Redirección).

En la página Launch Redirection (Iniciar redirección), elija el método de redirección de video o serie, si aparece, y, a continuación, haga clic en el botón Launch Remote Console (Iniciar consola remota).

Nota – De manera alternativa, se puede acceder a Oracle ILOM Remote Console desde el panel Actions (Acciones) de la página Summary (Resumen) en la interfaz web.

Aparece un cuadro de diálogo del programa Java Web Start.

2 En el cuadro de diálogo del programa Java Web Start, haga lo siguiente:

a. Haga clic en "Open with..." (Abrir con...) para especificar la ubicación del archivo JDK de 32 bits.

b. Haga clic en la casilla de verificación "Do this automatically for files like this from now on" (Hacer esto automáticamente para estos archivos a partir de ahora).

Nota – Si aparece un mensaje de advertencia de certificado que indica que el nombre del sitio no coincide con el nombre del certificado, haga clic en Run (Ejecutar) para continuar.

Aparece la ventana Oracle ILOM Remote Console.

Si desea obtener información adicional para redirigir dispositivos de KVMS con Oracle ILOM Remote Console, consulte "Inicio y uso de Oracle ILOM Remote Console " en la página 137.

Configuración opcional de un modo de bloqueo para proteger el escritorio del servidor host

Oracle ILOM proporciona la capacidad de bloquear el escritorio del servidor host cada vez que se desconecta una sesión de KVMS remoto. Esta función garantiza que, si un usuario de una sesión de KVMS cierra la sesión de KVMS antes de cerrar sesión en el escritorio del servidor host, los usuarios de sesiones de KVMS subsiguientes deban proporcionar sus credenciales de usuario para acceder al sistema.

Si desea obtener una descripción de las opciones del modo de bloqueo y la configuración de este modo en Oracle ILOM, consulte estos temas:

- Tabla 51
- "Bloqueo del escritorio del host al desconectar una sesión de KVMS remoto" en la página 135

TABLA 51 Opciones configurables de bloqueo del servidor host

Valores de la propiedad del modo de bloqueo	Descripción
Windows (`lock_mode=windows`)	La opción de bloqueo Windows se puede configurar en servidores host que ejecutan algún sistema operativo Microsoft Windows. Cuando la propiedad de modo de bloqueo de host se establece en `Windows`, Oracle ILOM funciona junto con el método abreviado de teclado estándar de Windows (CTRL-ALT-DEL) para bloquear el escritorio del sistema operativo Windows.
Custom (Personalizado) (`lock_mode=custom`)	La opción de bloqueo Custom se puede configurar para servidores host que ejecutan sistemas operativos Oracle Solaris, sistemas operativos Linux o sistemas operativos Microsoft Windows sin usar la secuencia de teclas CTRL-ALT-DEL. Cuando la propiedad de modo de bloqueo de host de Oracle ILOM está establecida en `Custom`, Oracle ILOM admite el uso de las siguientes secuencias de teclas para bloquear el escritorio. ■ Secuencias de teclas de bloqueo personalizadas admitidas por los sistemas operativos Oracle Solaris o Linux. La secuencia de teclas de bloqueo personalizada se debe definir en el sistema operativo host antes de activar la propiedad de modo de bloqueo Custom en Oracle ILOM. Si desea obtener instrucciones para crear una secuencia de teclas de bloqueo personalizada, consulte la documentación del proveedor del sistema operativo. ■ Una secuencia de teclas de bloqueo personalizada admitida por Windows, por ejemplo, el método abreviado de teclado de tecla de logotipo de Windows+L. La opción de modo de bloqueo Custom de Oracle ILOM no admite el método abreviado de teclado estándar de Windows que se utiliza para bloquear el escritorio (CTRL-ALT-DEL).
Disabled (Desactivado) (`lock_mode=disabled`)	Si la propiedad de modo de bloqueo de host está establecida en Disabled, que es el valor predeterminado, Oracle ILOM no bloquea automáticamente el escritorio del servidor host cuando finaliza la sesión de KVMS remoto.

▼ Bloqueo del escritorio del host al desconectar una sesión de KVMS remoto

Antes de empezar

- Para las configuraciones del modo de bloqueo personalizado, se debe definir la secuencia de teclas personalizada en el sistema operativo del servidor host antes de configurar la opción de modo de bloqueo personalizado en Oracle ILOM.
- Se necesita el rol Console (Consola) (c) para modificar las propiedades de bloqueo de host en Oracle ILOM.

1 Para configurar el valor de la propiedad de modo de bloqueo de host en Oracle ILOM, haga lo siguiente:

- **Web: haga clic en Remote Control (Control remoto) > KVMS. En la página KVMS Settings (Configuración de KVMS), haga clic en el cuadro de la lista Lock Mode (Modo de bloqueo) para seleccionar uno de los siguientes valores: Windows, Custom (Personalizado) o Disabled (Desactivado).**

- **CLI: escriba:**

  `set /SP/services/kvms lockmode=`*windows*|*custom*|*disabled*

  Si selecciona la opción Custom (Personalizado) para la propiedad Lock Mode (Modo de bloqueo), siga con el paso 2. Caso contrario, si está usando la interfaz web, siga con el paso 3.

2 Si, en el paso 1, configuró la propiedad Lock Mode (Modo de bloqueo) con la opción Custom (Personalizado), haga lo siguiente para especificar un modificador de bloqueo personalizado y una tecla de bloqueo personalizada:

- **Web: en la página KVMS Settings (Configuración de KVMS):**

  Haga clic en el cuadro de la lista Custom Lock Modifiers (Modificadores de bloqueo personalizados) y seleccione la secuencia de teclas personalizada definida en el sistema operativo del servidor host.

  Haga clic en el cuadro de la lista Custom Lock Key (Tecla de bloqueo personalizada) y seleccione una tecla de bloqueo personalizada.

- **CLI: escriba:**

  `set /SP/services/kvms lockmodifiers=`*value*

  `set /SP/services/kvms custom_lock_key=`*value*

Valores posibles para el modificador de bloqueo personalizado: l_alt, r_alt, l_shift, r_shift, l_ctrl, r_ctrl, l_gui, r_gui

Se pueden especificar hasta cuatro valores de modificador de bloqueo. Los modificadores se pueden separar con una coma.

Valores posibles para la tecla de bloqueo personalizada: esc, end, tab, ins, del, home, enter, space, break, backspace, pg_up, pg_down, scrl_lck, sys_rq, num_plus, num_minus, f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, a-z, 0-9, !, @, #, $, %, ^, &, *, (,), -,_, =, +,? |, ~, ?, [, {,], }, ;, :, ?, <, ., >, /,?

Vea el ejemplo (configuración de bloqueo de host) que se proporciona después de este procedimiento.

3 Para aplicar los cambios de propiedades hechos en la página KVMS Setting (Configuración de KVMS), haga clic en Save (Guardar).

Más información

Ejemplo de configuración de bloqueo de host:

Si se definió la siguiente secuencia de teclas de bloqueo personalizada (método abreviado de teclado) en el sistema operativo del servidor host:

Shift-Control-Backspace (Mayúsculas-Control-Retroceso)

Se configurarían las siguientes propiedades de bloqueo de KVMS en el SP de Oracle ILOM:

```
/SP/services/kvms

Properties:
    custom_lock_key = backspace
    custom_lock_modifiers = l_shift, l_ctrl
    lockmode = custom
    mousemode = absolute
    servicestate = enabled
```

Inicio y uso de Oracle ILOM Remote Console

Para iniciar y usar Oracle ILOM Remote Console basada en la GUI para la redirección de KVMS, lea estos temas:

- "Inicio y uso de Oracle ILOM Remote Console" en la página 137
- "Secuencia de teclas de alternancia para el control del teclado y el mouse " en la página 139
- "Opciones del menú Redirection (Redirección)" en la página 139
- "Opciones del menú Keyboard (Teclado)" en la página 141
- " Opciones del menú Devices (Dispositivos)" en la página 140

▼ Inicio y uso de Oracle ILOM Remote Console

Antes de empezar

- Asegúrese de que se cumplan los requisitos para el uso inicial: Tabla 50.
- Se necesita el rol Console (Consola) (c) para poder iniciar y usar Oracle ILOM Remote Console.
- Cuando se inicia Oracle ILOM Remote Console, se presentan las opciones de redirección de video y serie sólo para los SP de los servidores SPARC. Oracle ILOM Remote Console inicia automáticamente la redirección de video para los SP de los servidores x86.
- Para controlar el uso del teclado y el mouse entre Oracle ILOM Remote Console y el escritorio del host, consulte "Secuencia de teclas de alternancia para el control del teclado y el mouse " en la página 139.

- Al establecerse la sesión de redirección con el servidor host, se necesitan credenciales de usuario para iniciar sesión en el escritorio del sistema operativo host.

1 Para iniciar Oracle ILOM Remote Console, haga lo siguiente.

a. En la interfaz web de Oracle ILOM, seleccione Remote Control (Control remoto) > Redirection (Redirección).

b. En la página Launch Redirection (Iniciar redirección), haga clic en la opción de redirección presentada y, a continuación, haga clic en el botón Launch Remote Console (Iniciar consola remota).

Aparece el escritorio del servidor host redirigido en su estado actual. Por ejemplo, si el servidor host se está encendiendo, aparece una serie de mensajes de inicio; si el sistema operativo del servidor host está encendido, aparece un cuadro de diálogo de inicio de sesión del escritorio; si el servidor host no está encendido, aparece la pantalla vacía.

Nota – De manera alternativa, los usuarios del SP y el CMM pueden iniciar Oracle ILOM Remote Console desde el panel Actions (Acciones) de la página Summary (Resumen) de la interfaz web de Oracle ILOM.

---

2 Para detener, reiniciar o iniciar una nueva sesión de redirección, haga clic en el menú Redirection (Redirección) y seleccione la opción deseada del menú.

Si desea consultar una descripción de las opciones del menú, lea "Opciones del menú Redirection (Redirección)" en la página 139.

Consideraciones especiales:

- Cuando la sesión de KVMS se inicia desde un único SP del servidor host, aparece automáticamente una única vista de redirección.
- Es posible que haya varias vistas de redirección cuando: (1) se agrega manualmente una nueva sesión de KVMS o (2) la sesión inicial de KVMS se inicia desde la interfaz web del CMM (chasis). Una sesión de KVMS del CMM presenta una única vista de redirección para cada SP del servidor blade de la CPU gestionada por el chasis.

3 Para redirigir dispositivos, haga clic en el menú Devices (Dispositivos) y seleccione la opción deseada del menú.

Si desea consultar una descripción de las opciones del menú, lea " Opciones del menú Devices (Dispositivos)" en la página 140.

Consideraciones especiales:

- Si está instalando el software desde algún medio de distribución (CD/DVD), asegúrese de haber introducido el medio en la unidad redirigida del cliente local.
- Si está instalando el software desde una imagen ISO, asegúrese de que la imagen ISO esté almacenada en el cliente local o en un sistema de archivos de red compartido.

- En el caso de los usuarios de clientes de Oracle Solaris, antes de redirigir los dispositivos de almacenamiento, es preciso realizar el procedimiento siguiente:
  - Si está activada la aplicación Volume Manager, es preciso desactivarla.
  - Inicie sesión como `root` para iniciar la redirección del almacenamiento.

    De manera alternativa, para iniciar la redirección del almacenamiento, puede utilizar los siguientes comandos para asignar privilegios de root al procesador que ejecuta Oracle ILOM Remote Console:

    ```
    su to root
    ```

    ```
    ppriv -s +file_dac_read pid_javarconsole
    ```

4 **Para configurar los modos del teclado y las opciones de envío, haga clic en el menú Keyboard (Teclado) y seleccione la opción deseada del menú.**

Si desea consultar una descripción de las opciones del menú, lea "Opciones del menú Keyboard (Teclado)" en la página 141.

5 **Para salir de la consola remota, haga clic en la opción Quit (Salir) del menú Redirection (Redirección).**

Secuencia de teclas de alternancia para el control del teclado y el mouse

Use alguna de las siguientes secuencias de teclas de alternancia para controlar el uso del teclado y el mouse entre la aplicación Oracle ILOM Remote Console y el escritorio del cliente local.

Dispositivo del cliente local	Secuencia de teclas de alternancia
Mouse	Alt-m
Teclado	Alt-k

Opciones del menú Redirection (Redirección)

Opción del menú Redirection (Redirección)	Descripción
Start Redirection (Iniciar redirección) (predeterminado)	Haga clic en Start Redirection (Iniciar redirección) para activar el servicio de redirección. Esta opción está activada de manera predeterminada, por lo que el servicio de redirección se inicia automáticamente cuando aparece el cuadro de diálogo de Oracle ILOM Remote Console.

Opción del menú Redirection (Redirección)	Descripción
Restart Redirection (Reiniciar redirección)	La opción Restart Redirection (Reiniciar redirección) detiene y vuelve a iniciar la redirección activa de teclado, video, mouse y almacenamiento.
Stop Redirection (Detener redirección)	La opción Stop Redirection (Detener redirección) detiene la redirección activa de teclado, video, mouse y almacenamiento.
New Session (Nueva sesión)	Agrega una nueva sesión de redirección al conjunto de fichas actual.
Delete Session (Eliminar sesión)	Elimina una sesión de redirección del conjunto de fichas actual.

Opciones del menú Devices (Dispositivos)

Opción del menú Devices (Dispositivos)	Descripción
Keyboard (Teclado) (activado de manera predeterminada)	Haga clic en Keyboard (Teclado) para activar o desactivar el servicio de redirección del teclado del cliente local. Esta opción está activada de manera predeterminada, por lo que el servicio de redirección se inicia automáticamente para el teclado del cliente local.
Mouse (activado de manera predeterminada)	Haga clic en Mouse para activar o desactivar el servicio de redirección del mouse del cliente local. Esta opción está activada de manera predeterminada, por lo que el servicio de redirección se inicia automáticamente para el mouse del cliente local.
CD-ROM	Haga clic en CD-ROM para que el dispositivo de CD local actúe como si estuviera conectado directamente al servidor host remoto.
Floppy (Disquete)	Elija la opción Floppy (Disquete) para que el dispositivo de disquete local actúe como si estuviera conectado directamente al servidor host remoto. Esta opción no está disponible en los servidores host SPARC.
CD-ROM Image (Imagen de CD-ROM)	Seleccione CD-ROM Image (Imagen de CD-ROM) para especificar la ubicación de un archivo de imagen de CD-ROM que esté almacenado en el cliente local o en un recurso compartido de red.
Floppy Image (Imagen de disquete)	Seleccione Floppy Image (Imagen de disquete) para especificar la ubicación de un archivo de imagen de disquete que esté almacenado en el cliente local o en un recurso compartido de red. Esta opción no está disponible en los servidores host SPARC.

Opción del menú Devices (Dispositivos)	Descripción
Save as host defaults (Guardar como configuración predeterminada del host)	Haga clic en Save as host defaults (Guardar como configuración predeterminada del host) para configurar las opciones actualmente seleccionadas del menú Devices (Dispositivos) como configuración predeterminada.

Opciones del menú Keyboard (Teclado)

Nota – Oracle ILOM Remote Console admite el uso de todos los caracteres de los siguientes teclados internacionales: sueco, suizo-francés y finlandés.

Opción del menú Keyboard (Teclado)	Descripción
Auto-keybreak Mode (Modo de interrupción de teclas automático) (activado de forma predeterminada)	Haga clic en Auto-keybreak Mode (Modo de interrupción de teclas automático) para enviar de manera automática una interrupción de tecla después de cada pulsación de tecla. Esta opción puede ser útil para resolver problemas del teclado en conexiones de red lentas.
Stateful Key Locking (Bloqueo de teclas con estado)	Esta opción corresponde a Oracle Solaris con XSun u OSX. Haga clic en Stateful Key Locking (Bloqueo de teclas con estado) si el cliente local utiliza esta función. El bloqueo de teclas con estado se aplica a estas tres teclas de bloqueo: Bloq Mayús, Bloq Num y Bloq Despl.
Left Alt Key (Tecla Alt izquierda)	Esta opción no está disponible en los clientes de Windows. Pulse la tecla Alt izquierda para activar o desactivar la tecla Alt izquierda.
Right Alt Key / Alt Graph Key (Tecla Alt derecha o tecla Alt Gr)	Esta opción se utiliza en los teclados que no son estadounidenses. Haga clic en la tecla Alt derecha (tecla Alt Gr) para activarla o desactivarla. Si está activada, esta opción permite escribir el tercer carácter de una tecla.
F10	Haga clic en F10 para aplicar la tecla de función F10. Esta opción normalmente se aplica a la funcionalidad del BIOS de los servidores host x86.
Control Alt Delete (Control Alt Suprimir)	Pulse las teclas Control, Alt y Suprimir para enviar la secuencia de teclas Control-Alt-Supr.

Opción del menú Keyboard (Teclado)	Descripción
Control Space (Control Espacio)	Pulse Control y Espacio para enviar la secuencia Control-Espacio al servidor host, que activa la entrada del teclado.
Caps Lock (Bloqueo de mayúsculas)	Pulse la tecla Bloq Mayús para enviar la tecla Bloq Mayús al servidor host, que activa la entrada de datos con teclados rusos y griegos.

Configuración inicial para Oracle ILOM Storage Redirection CLI

Para configurar Oracle ILOM Storage Redirection CLI antes del primer uso, consulte estos temas:

- "Requisitos para el uso de Oracle ILOM Storage Redirection CLI" en la página 142
- "Registro del complemento de Java para el explorador IE de Windows y primer uso del servicio" en la página 143
- "Primer uso del servicio y registro del complemento de Java para el explorador Mozilla Firefox" en la página 145
- "Instalación del cliente de redirección de almacenamiento" en la página 146
- "Modificación opcional del puerto de red predeterminado 2121 para la redirección de almacenamiento" en la página 147

Requisitos para el uso de Oracle ILOM Storage Redirection CLI

Se deben cumplir los siguientes requisitos antes de utilizar Oracle ILOM Storage Redirection CLI por primera vez.

TABLA 52 Requisitos para el uso de Oracle ILOM Storage Redirection CLI

Requisito de configuración	Descripción
Entorno JRE 1.5	El cliente y el servicio de redirección de almacenamiento son aplicaciones de Java Web Start que requieren la instalación de Java Runtime Environment (1.5 o posterior) en el sistema del cliente local. Para descargar el software Java Runtime Environment (JRE) más actual, consulte `http://java.com`.

TABLA 52 Requisitos para el uso de Oracle ILOM Storage Redirection CLI *(Continuación)*

Requisito de configuración	Descripción
Registro del complemento JDK de 32 bits e inicio del servicio de redirección de almacenamiento	El servicio de redirección de almacenamiento se debe instalar localmente o se debe configurar para que se ejecute desde la interfaz web de Oracle ILOM. El complemento JDK de 32 bits de Java también debe estar registrado con el explorador web del cliente local. **Información relacionada**: ■ "Registro del complemento de Java para el explorador IE de Windows y primer uso del servicio" en la página 143 ■ "Primer uso del servicio y registro del complemento de Java para el explorador Mozilla Firefox" en la página 145
Instalación del cliente de redirección de almacenamiento	Después de registrar el complemento JDK de 32 bits con el explorador web del cliente local e iniciar el servicio de redirección de almacenamiento por primera vez, se debe instalar el cliente de redirección de almacenamiento en el sistema del cliente local. **Información relacionada**: ■ "Instalación del cliente de redirección de almacenamiento" en la página 146
Roles de usuario	Se necesita el rol Console (Consola) (c) en Oracle ILOM para iniciar y utilizar Oracle ILOM Storage Redirection CLI.
Puerto de comunicación TCP/IP requerido	De manera predeterminada, Oracle ILOM Storage Redirection CLI utiliza el puerto TCP/I: 2121 para comunicarse con el servidor host. **Información relacionada**: ■ "Modificación opcional del puerto de red predeterminado 2121 para la redirección de almacenamiento" en la página 147

▼ Registro del complemento de Java para el explorador IE de Windows y primer uso del servicio

Realice este procedimiento para: (1) registrar el complemento JDK de 32 bits de Java con el explorador IE de Microsoft Windows e (2) iniciar el servicio de redirección de almacenamiento por primera vez.

1. **En el cliente local de Windows, abra el Explorador de Windows (no Internet Explorer).**

2. **En el cuadro de diálogo Explorador de Windows, seleccione Herramientas > Opciones de carpeta y luego seleccione la ficha Tipos de archivo.**

3. **En la ficha Tipos de archivo, haga lo siguiente:**

   a. **En la lista de tipos de archivo registrados, seleccione el tipo de archivo JNLP y haga clic en Cambiar.**

b. **En el cuadro de diálogo Abrir con, haga clic en Examinar para seleccionar el archivo JDK de 32 bits almacenado en el sistema del cliente local.**

c. **Active la casilla de verificación "Usar siempre el programa seleccionado para abrir este tipo de archivos".**

d. **Haga clic en Aceptar.**

4 **Para iniciar el servicio de redirección de almacenamiento por primera vez, abra la interfaz web de Oracle ILOM y, a continuación, haga clic en Remote Control (Control remoto) > Redirection (Redirección) > Launch Service (Iniciar servicio).**

Aparece el cuadro de diálogo Opening Jnlpgenerator-cli (Apertura de Jnlpgenerator-cli).

5 **En el cuadro de diálogo Opening Jnlpgenerator-cli (Apertura de Jnlpgenerator-cli), elija una de las siguientes opciones para instalar el archivo o ejecutarlo desde la interfaz web:**

- **Install (Instalar): haga clic en "Save to disk," (Guardar en disco), especifique la ubicación del archivo de almacenamiento y, a continuación, haga clic en OK (Aceptar).**

- **Run (Ejecutar): haga clic en "Open it with" (Abrir con), elija el archivo JDK de 32 bits `javaws` (predeterminado) en el sistema local y, a continuación, haga clic en OK (Aceptar). Antes de ejecutarse el servicio de redirección de almacenamiento, aparece un cuadro de diálogo de advertencia de seguridad.**

Consideraciones especiales:

- Si elije ejecutar el archivo `Jnlpgenerator-cli` en lugar de instalarlo, los usuarios subsiguientes deberán iniciar el servicio de redirección de almacenamiento desde la interfaz web de Oracle ILOM antes de utilizar la consola de Oracle ILOM Storage Redirection CLI.
- Si elije ejecutar el archivo `Jnlpgenerator-cli` y también elije activar la casilla de verificación "*Always perform this action when handling this file type*," (Realizar siempre esta acción con este tipo de archivos), el cuadro de diálogo `Jnlpgenerator-cli` ya no estará disponible en el futuro para modificar el puerto de red de almacenamiento predeterminado. Por lo tanto, si en el futuro es necesario modificar el puerto de red predeterminado (2121), no active esta casilla de verificación.

6 **Realice una de las siguientes acciones para iniciar el servicio de redirección de almacenamiento:**

- **Run Service (Ejecutar servicio): en el cuadro de diálogo Security (Seguridad), haga clic en Run (Ejecutar) (o Yes [Sí]) para iniciar el servicio.**

- **Start service from command window or terminal (Iniciar servicio desde el terminal o la ventana de comandos): escriba la ubicación del archivo `Jnlpgenerator-cli` instalado seguida del comando `javaws rconsole.jnlp` para iniciar el servicio.**

  Ejemplo de sintaxis:

cd *jnlp file location* **javaws rconsole.jnlp**

Si el servicio de redirección de almacenamiento no se inicia, aparece un mensaje de error que informa que se produjo una condición de error. En otro caso, si no aparece un mensaje de error, el servicio se iniciará y esperará la entrada del usuario.

▼ Primer uso del servicio y registro del complemento de Java para el explorador Mozilla Firefox

Realice este procedimiento para: (1) iniciar por primera vez el servicio de redirección de almacenamiento y (2) registrar el complemento JDK de 32 bits de Java con el explorador web Mozilla Firefox.

1. **Inicie el servicio de redirección de almacenamiento desde la interfaz web de Oracle ILOM.**

   Haga clic en Remote Control (Control remoto) > Redirection (Redirección) > Launch Service (Iniciar servicio).

   Aparece un cuadro de diálogo para abrir el archivo `jnlpgenerator-cli`.

2. **En el cuadro de diálogo Opening Jnlpgenerator-cli (Apertura de Jnlpgenerator-cli), elija una de las siguientes opciones para instalar el servicio localmente o ejecutarlo desde la interfaz web:**

   - **Install (Instalar): haga clic en "Save to disk," (Guardar en disco), especifique la ubicación del archivo de almacenamiento y, a continuación, haga clic en OK (Aceptar).**
   - **Run (Ejecutar): haga clic en "Open it with" (Abrir con), elija el archivo JDK de 32 bits `javaws` (predeterminado) en el sistema local y, a continuación, haga clic en OK (Aceptar). Antes de ejecutarse el servicio de redirección de almacenamiento, aparece un cuadro de diálogo de advertencia de seguridad.**

   Consideraciones especiales:

   - Si elije ejecutar el archivo `Jnlpgenerator-cli` en lugar de instalarlo, los usuarios subsiguientes deberán iniciar el servicio de redirección de almacenamiento desde la interfaz web de Oracle ILOM antes de utilizar la consola de Oracle ILOM Storage Redirection CLI.
   - Si elije ejecutar el archivo `Jnlpgenerator-cli` y también elije activar la casilla de verificación "*Always perform this action when handling this file type*," (Realizar siempre esta acción con este tipo de archivos), el cuadro de diálogo `Jnlpgenerator-cli` ya no estará disponible en el futuro para modificar el puerto de red de almacenamiento predeterminado. Por lo tanto, si en el futuro es necesario modificar el puerto de red predeterminado (2121), no active esta casilla de verificación.

3 **Realice una de las siguientes acciones para iniciar el servicio de redirección de almacenamiento:**

- **Si el archivo `Jnlpgenerator-cli` está configurado para ejecutarse:**

  En el cuadro de diálogo Security (Seguridad), haga clic en Run (Ejecutar) (o Yes [Sí]) para iniciar el servicio.

- **Si el archivo `Jnlpgenerator-cli` está instalado localmente:**

  Escriba la ubicación del archivo jnlpgenerator-cli instalado seguida del comando **`javaws rconsole.jnlp`** para iniciar el servicio.

  Ejemplo de sintaxis:

  `cd` *jnlp file location* **`javaws rconsole.jnlp`**

  Si el servicio de redirección de almacenamiento no se inicia, aparece un mensaje de error que informa que se produjo una condición de error. En otro caso, si no aparece un mensaje de error, el servicio se iniciará y esperará la entrada del usuario.

Más información

Información relacionada:

- "Instalación del cliente de redirección de almacenamiento" en la página 146
- "Modificación opcional del puerto de red predeterminado 2121 para la redirección de almacenamiento" en la página 147

Instalación del cliente de redirección de almacenamiento

Realice el siguiente procedimiento para instalar el cliente de redirección de almacenamiento en el sistema del cliente local.

Nota – Esta instalación se debe realizar una única vez antes de utilizar por primera vez Oracle ILOM Storage Redirection CLI.

Antes de empezar

- El complemento de Java debe estar registrado y el servicio de redirección de almacenamiento se debe iniciar por primera vez.

  Para obtener instrucciones, consulte:

  - "Registro del complemento de Java para el explorador IE de Windows y primer uso del servicio" en la página 143
  - "Primer uso del servicio y registro del complemento de Java para el explorador Mozilla Firefox" en la página 145.

Para instalar el cliente de redirección de almacenamiento, siga estos pasos:

1 **En la interfaz web de Oracle ILOM, seleccione Remote Control (Control remoto) > Redirection (Redirección) > Download Client (Descargar cliente).**

Aparece un cuadro de diálogo para abrir el archivo StorageRedir.jar.

2 **En el cuadro de diálogo Opening StorageRedir.jar (Apertura de StorageRedir.jar), haga lo siguiente:**

- **Haga clic en "Save it to disk" (Guardar en disco) y, a continuación, haga clic en OK (Aceptar).**
- **En el cuadro de diálogo Save As (Guardar como), guarde el archivo `StorageRedir.jar` en una ubicación del sistema local.**

Más información

Información relacionada:

- "Modificación opcional del puerto de red predeterminado 2121 para la redirección de almacenamiento" en la página 147
- "Inicio y uso de Oracle ILOM Storage Redirection CLI" en la página 149

▼ Modificación opcional del puerto de red predeterminado 2121 para la redirección de almacenamiento

Si desea modificar el puerto de red predeterminado 2121 que Oracle ILOM utiliza para la redirección del almacenamiento, haga lo siguiente.

Antes de empezar

- Para el siguiente procedimiento, se necesita acceso al archivo Jnlpgenerator-cli.

Nota – Si el archivo `Jnlpgenerator-cli` para el servicio de redirección de almacenamiento se configuró para ejecutarse desde la interfaz web y el cuadro de diálogo *Opening Jnlpgenerator-cli* (Apertura de Jnlpgenerator-cli) se configuró para que no apareciera, no podrá utilizar el siguiente procedimiento para cambiar el puerto de red predeterminado para la redirección del almacenamiento.

- Se necesita el rol Console (Consola) (c) para ejecutar el servicio de redirección de almacenamiento desde la interfaz web de Oracle ILOM.

- Después de modificar el número de puerto predeterminado para la redirección del almacenamiento, los usuarios de este servicio de Oracle ILOM deberán especificar siempre el número de puerto no predeterminado al iniciar, detener o visualizar redirecciones de almacenamiento desde el terminal o la ventana de comandos.

Para modificar el puerto de red predeterminado 2121 para la redirección de almacenamiento, siga estos pasos:

1 **Para obtener acceso al archivo `Jnlpgenerator-cli`, realice una de las siguientes acciones:**

- **Si el archivo Jnlpgenerator-cli para la redirección de almacenamiento está instalado:**

  Use un editor de texto para abrir el archivo Jnlpgenerator-cli almacenado localmente.

- **Si el archivo Jnlpgenerator-cli para el servicio de redirección de almacenamiento está configurado para ejecutarse desde la interfaz web:**

  a. **En la interfaz web de Oracle ILOM, seleccione Remote Control (Control remoto) > Redirection (Redirección) > Launch Service (Iniciar servicio).**

     Aparece el cuadro de diálogo para abrir el archivo Jnlpgenerator-cli.

  b. **En el cuadro de diálogo `Opening Jnlpgenerator-cli` (Apertura de Jnlpgenerator-cli), haga clic en "Save to disk," (Guardar en disco) y, a continuación, haga clic en OK (Aceptar).**

  c. **En el cuadro de diálogo Save As (Guardar como), especifique la ubicación en la que desea almacenar el archivo y, a continuación, haga clic en OK (Aceptar).**

  d. **Con un editor de texto, abra el archivo `Jnlpgenerator-cli` almacenado en el sistema del cliente local.**

2 **Modifique el argumento del número de puerto que aparece en el archivo `Jnlpgenerator-cli` y, a continuación, guarde los cambios del archivo.**

Ejemplo de archivo:

```
<application-desc>
<argument>cli</argument>
<argument>2121</argument>
</application-desc>
```

Después de cambiar el puerto de red predeterminado 2121 y guardar los cambios en el archivo `Jnlpgenerator-cli` almacenado localmente, se debe especificar siempre el número de puerto no predeterminado al iniciar, detener o visualizar las redirecciones de almacenamiento desde el terminal o la ventana de comandos.

Inicio y uso de Oracle ILOM Storage Redirection CLI

Para iniciar y utilizar Oracle ILOM Storage Redirection CLI, consulte estos temas:

- "Inicio de Oracle ILOM Storage Redirection CLI y redirección de dispositivos de almacenamiento" en la página 149
- "Sintaxis de shell interactivo y no interactivo" en la página 154
- "Comandos y opciones de redirección de almacenamiento" en la página 154

▼ Inicio de Oracle ILOM Storage Redirection CLI y redirección de dispositivos de almacenamiento

Use el siguiente procedimiento para iniciar y utilizar la consola de Oracle ILOM Storage Redirection CLI.

Antes de empezar

- Asegúrese de que se cumplan los requisitos para el uso inicial: Tabla 52.
- Se necesita el rol Console (Consola) (c) para poder iniciar y usar Oracle ILOM Remote Console.
- Repase la sintaxis de los modos del shell y los comandos de redirección de almacenamiento:

  "Sintaxis de shell interactivo y no interactivo" en la página 154

  "Comandos y opciones de redirección de almacenamiento" en la página 154

Para iniciar la consola de Storage Redirection CLI y redirigir dispositivos de almacenamiento, siga estos pasos:

1 **Para iniciar el servicio de redirección de almacenamiento, realice una de las siguientes acciones:**

- **Para ejecutar el servicio de redirección de almacenamiento desde la interfaz web de Oracle ILOM:**

  a. **En la interfaz web de Oracle ILOM, seleccione Remote Control (Control remoto) > Redirection (Redirección) > Launch Service (Iniciar servicio).**

     Aparece el cuadro de diálogo para abrir el archivo Jnlpgenerator-cli.

  b. **En el cuadro de diálogo `Opening Jnlpgenerator-cli` (Apertura de Jnlpgenerator-cli), haga clic en "Open it with" (Abrir con), elija el archivo javaws (predeterminado) (archivo JDK de 32 bits) y, a continuación, haga clic en OK (Aceptar).**

  c. **En el cuadro de diálogo Warning Security (Advertencia de seguridad), haga clic en Run (Ejecutar) para iniciar el servicio de redirección de almacenamiento.**

d. Abra un terminal o una ventana de comandos en el sistema del cliente local para iniciar Oracle ILOM Storage Redirection CLI.

Si desea ver las instrucciones para iniciar Oracle ILOM Storage Redirection CLI, vaya al paso 2.

- **Para iniciar el servicio (instalado) de redirección de almacenamiento desde una ventana de comandos:**

a. Abra el terminal o la ventana de comandos en el sistema del cliente local.

Por ejemplo:

Sistemas Windows: desde el menú Inicio, haga clic en Ejecutar, escriba **`cmd`** y, a continuación, haga clic en Aceptar.

Sistemas Oracle Solaris o Linux: abra una ventana de terminal en el escritorio.

b. Vaya hasta la ubicación en la que está instalado el archivo `Jnlpgenerator-cli` y ejecute el comando `javaws rconsole.jnlp` para iniciar el servicio.

Por ejemplo:

`cd` *jnlp_file_location*/**`javaws rconsole.jnlp`**

2 Para iniciar la consola de Storage Redirection CLI desde el terminal o la ventana de comandos, realice uno de los siguientes procedimientos en función del modo de shell que esté utilizando.

Modo de shell	Descripción y procedimiento
Modo de shell interactivo	El modo interactivo es útil cuando hay que escribir una serie de comandos de redirección de almacenamiento. Para iniciar la consola de Storage Redirection CLI con un modo de shell interactivo, haga lo siguiente: a. En la interfaz de línea de comandos, use el comando cd para ir hasta el directorio donde se instaló el cliente de redirección de almacenamiento (`StorageRedir.jar`). Por ejemplo: **`cd`** *my_settings/storage_redirect_directory* b. Escriba el comando siguiente para iniciar Storage Redirection CLI. **`java -jar StorageRedir.jar`** Por ejemplo: C**`:\Documents and Settings\`***redirectstorage* **`java -jar StorageRedir.jar`** Aparece el indicador <*storageredir*>. **Nota –** Si utiliza Windows, debe especificar una letra mayúscula para la unidad de disco de destino. Por ejemplo, si la letra asignada a la unidad de disco de destino es c:, debe especificar C: en lugar de c:. **Consejo –** Escriba sólo un espacio antes de "`java`" y un espacio antes y uno después de "`-jar`". De no hacerlo así, el comando java -jar StorageRedir.jar generará un error. **Información relacionada**: ■ "Sintaxis de shell interactivo y no interactivo" en la página 154

Modo de shell	Descripción y procedimiento
Modo de shell no interactivo	El modo no interactivo es útil cuando hay que ejecutar un procedimiento por lotes o una secuencia de comandos. Para iniciar la consola de Storage Redirection CLI con un modo de shell no interactivo, haga lo siguiente: a. En·la·interfaz de línea de comandos, escriba el comando para iniciar Storage Redirection CLI (`java -jar StorageRedir.jar`) en el indicador del shell ($). `$ java -jar StorageRedir.jar` **Nota**: Si no configuró un entorno JAVA_HOME, quizá deba especificar la ruta completa al binario Java. Por ejemplo, si el paquete JDK se instaló en `/home/user_name/jdk`, tendría que escribir: `/home/user_name/jdk/bin/java -jar ....` b. Si Storage Redirection CLI no se inicia, se mostrará un mensaje de error detallado que explicará la condición del error. De lo contrario, Storage Redirection CLI está lista para que el usuario la utilice. **Nota –** Sin embargo, puede ejecutar varias consolas de Storage Redirection CLI mediante el comando de redirección de almacenamiento (`-jar StorageRedir.jar`) desde un terminal o una ventana de comandos local. **Consejo –** Escriba sólo un espacio antes y después de "`-jar`". De no hacerlo así, el comando `java -jar StorageRedir.jar` generará un error. **Información relacionada**: ■ "Sintaxis de shell interactivo y no interactivo" en la página 154 ■ "Comandos y opciones de redirección de almacenamiento" en la página 154

3 Para verificar que el servicio de redirección de almacenamiento se esté ejecutando, escriba el siguiente comando:

```
test-service
```

Aparece un mensaje que indica si el servicio de redirección está funcionando o ha generado un error.

Si desea leer una descripción de los comandos y la sintaxis del modo del shell, consulte estos temas:

- "Comandos y opciones de redirección de almacenamiento" en la página 154
- "Sintaxis de shell interactivo y no interactivo" en la página 154

4 Para iniciar la redirección de almacenamiento, escriba el siguiente comando `start` seguido de los subcomandos y las propiedades para el tipo de dispositivo de redirección, la ruta del dispositivo, el nombre de usuario y la contraseña del usuario del SP remoto, y la dirección IP del SP remoto.

Por ejemplo:

Nota – Los comandos que se indican en el siguiente ejemplo se deben introducir como cadena continua.

---

start -r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p non_default_storageredir_port] remote_SP_IP

Si desea leer una descripción de los comandos y la sintaxis del modo del shell, consulte estos temas:

- "Comandos y opciones de redirección de almacenamiento" en la página 154
- "Sintaxis de shell interactivo y no interactivo" en la página 154

5 **Para ver la redirección de almacenamiento activa, escriba el comando `list` seguido de los subcomandos y las propiedades de los puertos de redirección de almacenamiento no predeterminados que se estén utilizando y la dirección IP del SP del servidor host remoto.**

Por ejemplo:

list [-p non_default _storageredir_port] remote_SP

Si desea leer una descripción de los comandos y la sintaxis del modo del shell, consulte estos temas:

- "Comandos y opciones de redirección de almacenamiento" en la página 154
- "Sintaxis de shell interactivo y no interactivo" en la página 154

6 **Para detener la redirección de un dispositivo de almacenamiento, escriba el comando `stop` seguido de los comandos y las propiedades de: tipo de dispositivo de almacenamiento, nombre de usuario y contraseña del usuario del SP remoto, puerto de redirección de almacenamiento y dirección IP del SP del servidor host remoto.**

Por ejemplo:

stop -r redir_type -u remote_username [-s remote_user_password] [-p non_defult_storageredir_port] remote_SP

Si desea leer una descripción de los comandos y la sintaxis del modo del shell, consulte estos temas:

- "Comandos y opciones de redirección de almacenamiento" en la página 154
- "Sintaxis de shell interactivo y no interactivo" en la página 154

7 **Para mostrar la ayuda de la línea de comandos, escriba el siguiente comando:**

help

Aparece la información siguiente sobre la sintaxis y el uso de los comandos.

```
Uso:
```

```
list [-p storageredir_port] [remote_SP]

start -r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p
storageredir_port] remote_SP stop -r redir_type -u remote_username [-s
remote_user_password] [-p storageredir_port] remote_SP

stop-service [-p storageredir_port]

test-service [-p storageredir_port]

help

version

quit
```

Sintaxis de shell interactivo y no interactivo

A continuación se muestra la sintaxis necesaria para escribir los comandos de redirección de almacenamiento en ambos modos:

- **Sintaxis del modo de shell interactivo**

  `storageredir` *<command>* *<command_options>* *<sub_commands>* *<sub_command_options>*
- **Sintaxis del modo de shell no interactivo**

  `$ java -jar StorageRedir.jar` *<command>* *<command_options>* *<sub_commands>* *<sub_command_options>*

Comandos y opciones de redirección de almacenamiento

- Tabla 53
- Tabla 54
- Tabla 55
- Tabla 56

TABLA 53 Comandos de redirección de almacenamiento

Nombre del comando	Descripción
`java -jar StorageRedir.jar`	El comando `java -jar` se utiliza para iniciar el cliente de redirección de almacenamiento (`StorageRedir.jar`) desde un terminal o una ventana de comandos.
`storageredir`	El comando `storagedir` lleva a cabo todas las operaciones de redirección de almacenamiento.

TABLA 54 Opciones de comandos de redirección de almacenamiento

Nombre de la opción	Descripción
`- h`	La opción de comando `- h` muestra la información de ayuda de la línea de comandos.
`- v`	La opción de comando `- v` muestra la información de la versión del comando Java.

TABLA 55 Subcomandos de redirección de almacenamiento

Nombre del subcomando	Descripción
`list`	El subcomando `list` proporciona una lista de las redirecciones de almacenamiento actualmente activas en uno o todos los SP remotos. **Ejemplo de uso de la sintaxis**:`storageredir` **list** `[-p storageredir_port] [remote_SP]`
`start`	El subcomando `start` invoca la redirección especificada entre el host local y el servidor host remoto. Si no se proporciona la contraseña de autenticación, el sistema la solicitará. **Ejemplo de uso de la sintaxis**:`storageredir` **start** `-r redir_type -t redir_type_path -u remote_username [-s` `[-p storageredir_port] remote_SP` **Nota –** Debe especificar un rol válido Admin (Administrador) (a) o Console (Consola) (c) en Oracle ILOM para iniciar la redirección del dispositivo de almacenamiento en un servidor remoto.
`stop`	El subcomando `stop` detiene la redirección especificada entre el host local y el servidor host remoto. Si no se proporciona la contraseña de autenticación, el sistema la solicitará. **Ejemplo de uso de la sintaxis**:`storageredir` **stop** `-r redir_type -u remote_username [-s remote_user_password] [-p storageredir_port] remote_SP` **Nota –** Debe especificar un rol válido Admin (Administrador) (a) o Console (Consola) (c) en Oracle ILOM para detener la redirección del dispositivo de almacenamiento en un servidor remoto.
`test-service`	El subcomando `test-service` comprueba si la conexión del servicio de redirección de almacenamiento está activa en el host local. **Ejemplo de uso de la sintaxis**:`storageredir` **test-service** `[-p storageredir_port]`
stop-service	El subcomando `stop-service` detiene la conexión del servicio de redirección de almacenamiento al servidor host remoto. **Ejemplo de uso de la sintaxis**:`storageredir` **stop-service** `[-p storageredir_port]`

TABLA 56 Opciones de subcomandos de redirección de almacenamiento

Nombre de la opción del subcomando	Descripción
`-r` *redir_type*	La opción `-r` *redir_type* identifica el tipo de medio de almacenamiento que se está redirigiendo. Los valores válidos para *redir_type* incluyen: ■ Sintaxis del dispositivo de CD-ROM: `-r cdrom` ■ Sintaxis de la imagen de CD-ROM: `-r cdrom_img` ■ Sintaxis del dispositivo de disquete: `-r floppy` ■ Sintaxis de la imagen de disquete: `-r floppy_img`
`-t` *redir_type_path*	La opción `-t` *redir_type_path* identifica la ruta completa de la ubicación en la que está almacenado o montado el medio de redirección de almacenamiento. **Ejemplo**: `-t` /home/username/JRC_Test_Images/CDROM.iso
`-u` *remote_username*	La opción `-u` *remote_username* identifica el nombre de usuario requerido para iniciar sesión en el SP de Oracle ILOM. Ejemplo: `-u` *john_smith* **Nota –** Cualquier cuenta de usuario válida en Oracle ILOM puede instalar o iniciar el servicio o el cliente de redirección de almacenamiento en el sistema local. No obstante, se debe especificar un rol Admin (Administrador) (a) o Console (Consola) (c) válido en Oracle ILOM para iniciar o detener la redirección del dispositivo de almacenamiento en un servidor remoto.
`-s` *remote_user_password*	La opción `-s` *remote_user_password* identifica la contraseña requerida para iniciar sesión en el SP de Oracle ILOM. **Ejemplo**: `-s` *my_password* Si este comando de contraseña no se especifica en la línea de comandos, el sistema la solicitará automáticamente.
`-p` *storageredir_port*	La opción `-p` *storageredir_port* identifica el puerto de comunicación de redirección de almacenamiento en el host local. El puerto predeterminado que se proporciona es el 2121. **Ejemplo**: `-p 2121`

Inicio y detención de una sesión de redirección serie del host

Además de Oracle ILOM Remote Console y Oracle ILOM Storage Redirection CLI, Oracle ILOM permite iniciar una sesión de redirección serie basada en texto para el sistema operativo del servidor host.

Los usuarios con rol Console (Consola) (c) de Oracle ILOM pueden iniciar y detener consolas de redirección serie de hosts desde la CLI. Después de iniciar la sesión de redirección, se necesitan credenciales de usuario del host para poder acceder al sistema operativo host. Antes de detener la sesión de redirección desde Oracle ILOM, los usuarios del host deben cerrar sesión en el sistema operativo host.

Si desea obtener instrucciones adicionales para iniciar y detener consolas serie del host desde la CLI, lea el siguiente procedimiento.

▼ Inicio de la redirección de consolas serie e inicio de sesión en el sistema operativo del servidor host

Antes de empezar

- Se necesita el rol Console (Consola) (c) en Oracle ILOM para iniciar una sesión de redirección serie para el sistema operativo del servidor host.
- Se necesitan credenciales de usuario del servidor host para obtener acceso al sistema operativo host. Los usuarios deben cerrar sesión en el sistema operativo host antes de finalizar la sesión de redirección del host desde Oracle ILOM.
- Las sesiones de redirección serie de hosts se pueden iniciar solamente desde la CLI de un SP de Oracle ILOM.

1. **Para iniciar una consola de redirección serie de hosts desde la CLI del SP de Oracle ILOM, escriba:**

   `start /host/console`

   Aparece un mensaje que le indica que especifique las credenciales de usuario.

2. **Escriba las credenciales de usuario requeridas para acceder al sistema operativo del servidor host.**

   Ya inició sesión en el sistema operativo del servidor host mediante la consola serie del host.

Nota – Para emitir comandos estándar de la CLI de Oracle ILOM, primero debe salir de la consola serie del host.

---

3. **Para finalizar la sesión de redirección del host, cierre sesión en el sistema operativo del servidor host y, a continuación, pulse estas teclas para finalizar la sesión de la consola serie del host: `ESC` y `(`.**

Nota – Para enviar una interrupción al host, pulse la tecla Esc y escriba la letra B mayúscula.

Configuración de acciones de gestión del servidor host

Descripción	Vínculos
Consulte esta sección si desea obtener descripciones de las propiedades configurables del CMM y el SP para el control de energía del host.	■ "Control de energía del host para el chasis del sistema blade o el servidor " en la página 160
Consulte esta sección si desea obtener descripciones de las propiedades de diagnóstico configurables del SP.	■ "Configuración de la ejecución de pruebas de diagnóstico del host" en la página 161
Consulte esta sección si desea obtener descripciones de las propiedades configurables del SP de servidores x86 para el siguiente dispositivo de inicio.	■ "Configuración del siguiente dispositivo de inicio en servidores host x86" en la página 165
Consulte esta sección si desea obtener descripciones de las propiedades del SP de servidores SPARC para el control del host.	■ "Configuración del comportamiento de inicio en servidores host SPARC" en la página 166
Consulte esta sección si desea obtener descripciones de las propiedades configurables del modo de inicio del SP de servidores SPARC para OpenBoot y LDoms.	■ "Anulación del modo de inicio de host SPARC" en la página 170
Consulte esta sección si desea obtener descripciones de las propiedades configurables de inicio del SP de servidores SPARC para el dominio del host y ver una lista de los valores actuales de LDom.	■ "Gestión de dominios de host SPARC" en la página 172
Consulte esta sección si desea obtener descripciones de los valores de las propiedades configurables del SP de servidores SPARC para el estado del selector del host.	■ "Configuración del estado del selector para hosts SPARC " en la página 174
Consulte esta sección si desea obtener descripciones de los valores de las propiedades configurables del SP de servidores SPARC para el estado del módulo de plataforma de confianza del host.	■ "Configuración del estado del módulo de plataforma de confianza para hosts SPARC " en la página 175

Información relacionada

- "Mantenimiento de parámetros de configuración del BIOS en un servidor x86" en la página 221

Control de energía del host para el chasis del sistema blade o el servidor

Oracle ILOM proporciona un conjunto de parámetros que permiten a los administradores del sistema controlar el estado de energía de un sistema de chasis blade o un servidor host.

Los administradores del sistema pueden emitir los comandos de control de energía desde la interfaz web o la CLI de Oracle ILOM. Si desea obtener más información sobre cada comando de control de energía, consulte la siguiente tabla.

TABLA 57 Comandos de control remoto de energía para dispositivos gestionados del host

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** <*command*> `/System`
- **Web:** Host Management (Gestión de host) > Power Control (Control de energía)
- **Rol de usuario:** Admin (Administrador) (a)

Requisito:

- Para aplicar la opción de energía seleccionada en la interfaz web, debe hacer clic en Save (Guardar).

Web	CLI	Se aplica a:	Descripción
Reset (Restablecer)	■ SP de x86: `reset /System` ■ SPARC: `reset -force /System`	■ Cualquier servidor gestionado	Use la opción Reset (Restablecer) para hacer que el servidor gestionado se apague y se vuelva a encender, pero mantener los componentes del sistema encendidos (por ejemplo, las unidades de disco).
Graceful Reset (Restablecimiento controlado)	■ `reset /System`	■ Sólo servidor gestionado SPARC	Use la opción Graceful Reset (Restablecimiento controlado) para apagar de manera controlada el sistema operativo host antes de apagar y volver a encender el servidor gestionado.
Immediate Power Off (Apagado inmediato)	■ `stop -force /System`	■ Cualquier servidor gestionado o chasis de sistema blade	Use la opción Immediate Power Off (Apagado inmediato) para apagar directamente el dispositivo gestionado.
Graceful Shutdown and Power Off (Cierre controlado y apagado)	■ `stop /System`	■ Cualquier servidor gestionado o chasis de sistema blade	Use la opción Graceful Shutdown and Power Off (Cierre controlado y apagado) para cerrar de manera controlada el sistema operativo host antes de apagar el dispositivo gestionado.

TABLA 57 Comandos de control remoto de energía para dispositivos gestionados del host *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI**: <*command*> **/System**
- **Web**: **Host Management (Gestión de host) > Power Control (Control de energía)**
- **Rol de usuario**: **Admin (Administrador) (a)**

Requisito:
- Para aplicar la opción de energía seleccionada en la interfaz web, debe hacer clic en Save (Guardar).

Web	CLI	Se aplica a:	Descripción
Power On (Encendido)	■ `start /System`	■ Cualquier servidor gestionado o chasis de sistema blade	Use la opción Power On (Encendido) para aplicar energía completa al dispositivo gestionado.
Power Cycle (Apagado y encendido)	■ `stop /System` ■ `start /System`	■ Cualquier servidor gestionado	Use la opción Power Cycle (Apagado y encendido) para apagar el sistema y todos sus componentes, y luego aplicar energía completa a todos los componentes del sistema.

Configuración de la ejecución de pruebas de diagnóstico del host

Oracle ILOM proporciona un conjunto de propiedades de diagnóstico específicas de cada servidor que permiten a los administradores del sistema controlar si se ejecutan pruebas de diagnóstico del sistema en el inicio. Estas propiedades de diagnóstico se pueden configurar desde la CLI o la interfaz web de Oracle ILOM. Si desea obtener información adicional sobre estas propiedades, consulte las siguientes tablas:

- Tabla 58
- Tabla 59

TABLA 58 Propiedades de diagnóstico del SP de servidores x86

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** `/HOST`
- **Web**: Host Management (Gestión de host) > Diagnostics (Diagnóstico)
- **Rol de usuario**: Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades de diagnóstico)

Requisito:

- Para aplicar las modificaciones de las propiedades de diagnóstico en la interfaz web, debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Run Diagnostics on Boot (Ejecutar diagnóstico al iniciar) (/diag/state=*disabled*|*enabled*|*extended*|*manual*)	Disabled (Desactivado)	*Disabled*| *Enabled* |*Extended* |*Manual* ■ Disabled (Desactivado): las pruebas de diagnóstico de PC-Check no se ejecutan cuando se enciende el servidor x86. ■ Enabled (Activado): las pruebas de diagnóstico básicas de PC-Check se ejecutan cuando se enciende el servidor x86 y se completan en aproximadamente 3 minutos. ■ Extended (Extendido): las pruebas de diagnóstico extendidas de PC-Check se ejecutan cuando se enciende el servidor x86 y se completan en aproximadamente 20 minutos. ■ Manual: las pruebas de diagnóstico de PC-Check se ejecutan en el modo manual cuando se reinicia el servidor. Al encender el servidor, aparece el menú de las pruebas de diagnóstico de PC-Check, desde donde se pueden activar las pruebas de manera manual. **Sintaxis de la CLI para la ejecución de las pruebas de diagnóstico en el inicio:** **`set /HOST/diag state=`***disabled*|*enabled*|*extended*|*manual*
Generate NMI button (Botón Generar NMI) `(generate_host_nmi=true)`	Ningún valor	Esta opción, si está activada, envía una interrupción no enmascarable al sistema operativo host. **Nota** – En función de la configuración del sistema operativo host, esta acción puede hacer que el sistema operativo: falle, deje de responder o espere la entrada de un depurador externo. **Sintaxis de la CLI para generar una NMI:** **`set /HOST/generate_host=true`**

TABLA 59 Propiedades de diagnóstico del SP de servidores SPARC

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** `/HOST/diag`
- **Web:** Host Management (Gestión de host) > Diagnostics (Diagnóstico)
- **Rol de usuario:** Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades de diagnóstico)

Requisito:

- Para aplicar las modificaciones de las propiedades de diagnóstico en la interfaz web, debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Trigger (Disparador) (`trigger=`*error-reset*|*hw-change*|*power-on-resets*)	HW-Change (Cambio de hardware)	*Power-On*| *HW-Change*|*Error-Reset* Especifique uno o varios de los siguientes disparadores para generar la ejecución de las pruebas automáticas de encendido (POST). ■ Power On (Encendido): si está activado, se ejecutan las pruebas automáticas de encendido (POST) cuando se enciende el servidor SPARC. ■ HW-Change (Cambio de hardware): si está activado, se ejecutan las pruebas automáticas de encendido (POST) al iniciar cuando se produce alguno de los siguientes cambios de hardware: reemplazo de FRU, extracción de cubierta o ciclo de apagado y encendido. ■ Error-reset (Restablecimiento por error): si está activado, se ejecutan las pruebas automáticas de encendido (POST) después de producirse un restablecimiento de energía invocado por un error. **Sintaxis de la CLI para el disparador:** **`set /HOST/diag/trigger=`***error-reset*|*hw-change*|*power-on-resets*
Trigger Levels (Niveles de disparadores) (`power_on_level=|hw_change_level=|errror_reset_level=`)	Max (Máximo)	*Max* |*Min* Configure de manera independiente un nivel de prueba para cada disparador activado. ■ Max (Máximo): si está activado, se ejecuta el nivel máximo de pruebas de diagnóstico. ■ Min (Mínimo): si está activado, se ejecuta el nivel mínimo de pruebas de diagnóstico. **Sintaxis de la CLI para los niveles de disparadores:** **`set /HOST/diag/error_reset_level=`***min*|*max* **`hw_change_level=`***min*|*max* **`power_on_level=`***min*|*max*

TABLA 59 Propiedades de diagnóstico del SP de servidores SPARC *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** `/HOST/diag`
- **Web:** Host Management (Gestión de host) > Diagnostics (Diagnóstico)
- **Rol de usuario:** Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades de diagnóstico)

Requisito:

- Para aplicar las modificaciones de las propiedades de diagnóstico en la interfaz web, debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Trigger Verbosity (Nivel de detalle del disparador) `(power_on_verbosity=|hw_change_verbosity=|error_reset_verbosity=)`	Min (Mínimo)	*Normal* |*Min* |*Max*| *Debug* |*None* Configure de manera independiente un nivel de informe para cada dispositivo activado: ■ Normal: si está activado, Oracle ILOM genera una cantidad moderada de información de depuración para la consola del sistema. La salida incluye el nombre y los resultados de cada ejecución de las pruebas. ■ Min (Mínimo): si está activado, Oracle ILOM genera una cantidad limitada de salida en la consola del sistema (valor predeterminado). ■ Max (Máximo): si está activado, Oracle ILOM genera información de depuración de cada paso de las pruebas POST para la consola del sistema. ■ Debug (Depuración): si está activado, Oracle ILOM genera información exhaustiva de depuración para la consola del sistema. La salida incluye los nombres de los componentes que se analizaron y los resultados de cada prueba ejecutada. ■ None (Ninguno): si está activado, Oracle ILOM desactiva la generación de información de depuración para la consola del sistema. **Sintaxis de la CLI para el nivel de detalle del disparador:** **set** **/HOST/diag/error_reset_verbosity=***normal*|*min*|*max*|*debug*|*none* **hw_change_verbosity=***normal*|*min*|*max*|*debug*|*none* **power_on_verbosity=***normal*|*min*|*max*|*debug*|*none*

TABLA 59 Propiedades de diagnóstico del SP de servidores SPARC *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI del SP:** `/HOST/diag`
- **Web:** Host Management (Gestión de host) > Diagnostics (Diagnóstico)
- **Rol de usuario:** Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades de diagnóstico)

Requisito:
- Para aplicar las modificaciones de las propiedades de diagnóstico en la interfaz web, debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Mode (Modo) (`mode=`)	Normal	*Off* |*Normal* Configure un modo para activar o desactivar la ejecución de las pruebas automáticas de encendido para todos los disparadores activados. ■ Off (Desactivado): se impide la ejecución de las pruebas automáticas de encendido (POST) para todos los disparadores activados. ■ Normal: las pruebas automáticas de encendido (POST) se ejecutan para todos los disparadores activados (valor predeterminado). **Sintaxis de la CLI para el modo**: **`set /HOST/diag/mode=`***normal*|*off*

Configuración del siguiente dispositivo de inicio en servidores host x86

Oracle ILOM proporciona un conjunto de propiedades de servidores x86 que permiten a los administradores del sistema configurar el siguiente dispositivo de inicio en el servidor host. Sin embargo, estas propiedades configurables del dispositivo de inicio de Oracle ILOM se aplican solamente en el siguiente encendido del servidor x86.

Nota – Una vez que el sistema se enciende y se inicia el dispositivo de inicio especificado por el usuario de Oracle ILOM, el sistema regresa a las propiedades de dispositivo de inicio configuradas en la utilidad BIOS del sistema.

Los administradores del sistema pueden configurar la propiedad del siguiente dispositivo de inicio del servidor x86 desde la CLI o la interfaz web de Oracle ILOM. Si desea obtener más información sobre estas propiedades del siguiente dispositivo de inicio en servidores x86, consulte la siguiente tabla.

TABLA 60 Configuración de la propiedad del siguiente dispositivo de inicio en servidores x86 gestionados

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** `/SP/HOST/boot_device=`
- **Web del SP:** Host Management (Gestión de host) > Host Control (Control de host) > Next Boot Device (Siguiente dispositivo de inicio)
- **Rol de usuario:** Reset and Host Control (Restablecimiento y control del host) (r)

Requisito:

- Para aplicar una opción de siguiente dispositivo de inicio en la interfaz web, debe hacer clic en Save (Guardar).

Valor de la propiedad	Descripción
Default (Use BIOS Settings) (Valor predeterminado [usar la configuración del BIOS]) (`boot_device=default`)	Configure la propiedad Default (Use BIOS Settings) (Valor predeterminado [usar la configuración del BIOS]) para que el sistema x86 se inicie desde el primer dispositivo actualmente configurado en el orden de inicio del BIOS del sistema. Para configurar las propiedades configurables del host desde la CLI, ejecute el comando set (`set /Host property_name=`*value*).
PXE (`boot_device=pxe`)	Configure la propiedad PXE para que se omita de manera temporal el orden de inicio del BIOS del sistema y se inicie el sistema x86 por medio de la red con la especificación de inicio PXE.
Disk (Disco) (`boot_device=disk`)	Configure la propiedad Disk (Disco) para que se omita de manera temporal el orden de inicio del BIOS del sistema y se inicie desde el primer dispositivo de disco determinado por el primer disco en el orden de inicio de la utilidad BIOS.
Diagnostic (Diagnóstico) (`boot_device=diagnostic`)	Configure la propiedad Diagnostic (Diagnóstico) para que se omita de manera temporal el orden de inicio del BIOS del sistema y se inicie el sistema desde la partición de diagnóstico si está configurada.
CDROM (`boot_device=cdrom`)	Configure la propiedad CDROM para que se omita de manera temporal el orden de inicio del BIOS del sistema y se inicie el sistema desde el dispositivo de CD-ROM o DVD conectado.
BIOS (`boot_device=bios`)	Configure la propiedad BIOS para que se omita de manera temporal el orden de inicio del BIOS y se inicie el sistema desde el menú de configuración de la utilidad BIOS.

Configuración del comportamiento de inicio en servidores host SPARC

Oracle ILOM proporciona un conjunto de propiedades de servidores SPARC que permiten a los administradores del sistema ver la información de control del host y, de manera opcional, configurar propiedades para controlar el comportamiento del sistema en el inicio.

Los administradores del sistema pueden ver la información de control del host o establecer propiedades configurables de inicio del servidor SPARC desde la CLI o la interfaz web de Oracle ILOM. Si desea obtener información detallada sobre estas propiedades, consulte la siguiente tabla.

TABLA 61 Información de control de host y propiedades de inicio en servidores gestionados SPARC

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** `/HOST property_name`
- **Web:** Host Management (Gestión de host) > Host Control (Control de host)
- **Rol de usuario:** Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades configurables del host)

Requisito:

- Para aplicar las modificaciones en las propiedades desde la página web Host Control (Control de host), debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Host Control Information (Información de control de host) `/HOST`	Propiedades de sólo lectura	Vea la información de control de host de servidores SPARC para: ■ MAC Address (Dirección MAC): muestra la dirección MAC de Ethernet asignada al dispositivo gestionado. ■ Hypervisor Version (Versión de hipervisor): muestra la versión del firmware Hypervision. ■ OBP: muestra la versión del firmware OpenBoot PROM (OBP). ■ POST Version (Versión de POST): muestra la versión actual de POST. ■ SysFW Version (Versión de SysFw): muestra la versión actualmente instalada del firmware Oracle ILOM. ■ Host Status (Estado del host): muestra el estado de energía actual del sistema operativo host. **Sintaxis de la CLI para la información de control de host**: **`show /HOST`**
Auto Run On Error (Ejecución automática al producirse un error) (`autorunonerror=false|true`)	False, desactivada	*False*| *True* Configure esta opción para indicar a Oracle ILOM que continúe con el inicio del servidor SPARC si se produce un error de inicio no fatal. **Sintaxis de la CLI para la ejecución automática al producirse un error**: **`set /HOST autorunonerror=`***true*|*false*

TABLA 61 Información de control de host y propiedades de inicio en servidores gestionados SPARC *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** `/HOST property_name`
- **Web**: Host Management (Gestión de host) > Host Control (Control de host)
- **Rol de usuario**: Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades configurables del host)

Requisito:

- Para aplicar las modificaciones en las propiedades desde la página web Host Control (Control de host), debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Auto Restart Policy (Política de reinicio automático) (`autorestart=`)	Restablecer	*Reset* |*Dump Core*|*None* Configure esta opción para indicar a Oracle ILOM la acción que debe realizar si el sistema operativo host se bloquea. ■ Reset (Restablecer) (valor predeterminado): Oracle ILOM intenta restablecer la energía en el servidor SPARC cuando el temporizador de vigilancia de Oracle Solaris caduca. ■ None (Ninguno): Oracle ILOM sólo emite una advertencia. ■ Dump Core (Volcar núcleo): Oracle ILOM intenta forzar un volcado del núcleo central del sistema operativo cuando el temporizador de vigilancia de Oracle Solaris caduca. **Sintaxis de la CLI para la política de reinicio automático**: **`set /HOST autorestart=`***reset*|*dumpcore*|*none*
Boot Timeout (Tiempo de espera de inicio) (`boottimeout=`)	0, temporizador desactivado	Número entero entre *0* y *36000* segundos Configure un valor de tiempo de espera para el temporizador de inicio en el servidor SPARC. **Sintaxis de la CLI para el tiempo de espera de inicio**: **`set /HOST bootimeout=`***0 to 360000*
Boot Restart Policy (Política de reinicio de inicio) (`bootrestart=`)	Ninguno, política desactivada	*None*|*Reset* Configure esta opción para indicar a Oracle ILOM si debe reiniciar el servidor SPARC si se agota el tiempo de espera del sistema. **Sintaxis de la CLI para la política de reinicio de inicio**: **`set /HOST bootrestart=`***reset*|*none*

TABLA 61 Información de control de host y propiedades de inicio en servidores gestionados SPARC *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI del SP:** `/HOST property_name`
- **Web:** Host Management (Gestión de host) > Host Control (Control de host)
- **Rol de usuario:** Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades configurables del host)

Requisito:
- Para aplicar las modificaciones en las propiedades desde la página web Host Control (Control de host), debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Max Boot Fails Allowed (Cantidad máxima permitida de errores de inicio) (`maxbootfails=`)	3 intentos	Número entero entre *0* y *10000* intentos. Configure la cantidad máxima permitida de intentos si se produce un error del proceso de inicio de Oracle Solaris. Si el host no se inicia satisfactoriamente dentro la cantidad de intentos indicada en la propiedad de cantidad máxima de errores de inicio, se apagará o experimentará un ciclo de apagado y encendido (según la configuración de la opción de recuperación de error de inicio). En cualquier caso, el tiempo de espera del inicio es de 0 (cero segundos), lo cual desactiva posteriores intentos de reinicio del host. **Sintaxis de la CLI para la cantidad máxima permitida de errores de inicio**: **`set /HOST bootrestart=`***0 to 10000*
Boot Fail Recovery (Recuperación de error de inicio) (`bootfailrecovery=`)	Apagado	*Powercycle* |*Poweroff* | *None* Configure esta propiedad para indicar a Oracle ILOM la acción que debe realizar si el proceso de inicio no se pudo completar después de haber alcanzado la cantidad máxima de intentos de inicio. ■ Poweroff (Apagado) (valor predeterminado): Oracle ILOM apaga el servidor SPARC cuando se alcanza la cantidad máxima de intentos de inicio. ■ Powercycle (Apagado y encendido): Oracle ILOM apaga el servidor SPARC y vuelve a encenderlo cuando se alcanza la cantidad máxima de intentos de inicio. ■ None (Ninguno): la propiedad Boot Fail Recovery (Recuperación de error de inicio) está desactivada. **Sintaxis de la CLI para la recuperación de error de inicio**: **`set /HOST bootfailrecovery`**=*off*|*none*|*powercycle*

Anulación del modo de inicio de host SPARC

Oracle ILOM proporciona un conjunto de propiedades de modo de inicio del host que permite a los administradores del sistema anular el método de inicio predeterminado para iniciar el sistema operativo host en el servidor SPARC.

El propósito de las propiedades del modo de inicio del host de Oracle ILOM es ayudar a resolver configuraciones dañadas del modo de inicio con OpenBoot o LDoms. Las propiedades del modo de inicio, si se configuran en Oracle ILOM, se aplican solamente a un único inicio y expiran antes de que transcurran 10 minutos si no se vuelve a encender el servidor host SPARC.

Los administradores del sistema pueden utilizar la CLI o la interfaz web de Oracle ILOM para configurar las propiedades del modo de inicio del host. Si desea obtener información detallada sobre estas propiedades, consulte la siguiente tabla.

TABLA 62 Propiedades del modo de inicio del host para servidores host SPARC

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI del SP:** `/HOST/bootmode`
- **Web del SP:** Host Management (Gestión de host) > Host Boot Mode (Modo de inicio de host)
- **Rol de usuario**: Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades configurables del modo de inicio)

Requisito:
- Para aplicar los cambios de las propiedades del modo de inicio en la página Host Boot Mode Settings (Configuración del modo de inicio del host), debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
State (Estado) (state=)	Normal	*Normal* | *Reset NVRAM* Configure esta opción para indicar a Oracle ILOM la acción que debe realizar cuando se vuelve a encender el servidor SPARC. ■ Normal: Oracle ILOM conserva las propiedades actuales de las variables de NVRAM. ■ Reset NVRAM (Restablecer NVRAM): Oracle ILOM vuelve a configurar todas las variables de OpenBoot con los valores predeterminados cuando se vuelve a encender el servidor SPARC. **Sintaxis de la CLI para el estado del modo de inicio del host**: **`set /HOST/bootmode state=`***normal*|*reset_nvram*

TABLA 62 Propiedades del modo de inicio del host para servidores host SPARC *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** `/HOST/bootmode`
- **Web del SP:** **Host Management (Gestión de host) > Host Boot Mode (Modo de inicio de host)**
- **Rol de usuario:** **Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades configurables del modo de inicio)**

Requisito:

- Para aplicar los cambios de las propiedades del modo de inicio en la página Host Boot Mode Settings (Configuración del modo de inicio del host), debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Expiration Date (Fecha de caducidad) `(expires=)`	Ningún valor, propiedad de sólo lectura	Las propiedades del modo de inicio caducan antes de que transcurran 10 minutos o cuando se vuelve a encender el servidor SPARC (lo que suceda primero). Las propiedades Config (Configuración) y Script (Secuencia de comandos) de LDOM no caducan y se borran cuando el servidor se vuelve a encender o cuando se borran los valores de manera manual. **Sintaxis de la CLI para el estado del modo de inicio del host**: **`show /HOST/bootmode`**
Script (Secuencia de comandos) `(script=)`	Ningún valor	Hasta 64 bytes de longitud. La secuencia de comandos controla el método de inicio del firmware OpenBoot PROM del servidor host SPARC. La secuencia de comandos se lee cuando: (1) la propiedad State (Estado) está establecida en Reset NVRAM (Restablecer NVRAM), (2) se vuelve a encender el servidor SPARC y (3) se restablecen los valores predeterminados de las variables de OpenBoot. **Nota –** El personal del servicio de asistencia puede indicarle que especifique una secuencia de comandos para la resolución del problema. Las capacidades de la secuencia de comandos no están completamente documentadas y se emplean fundamentalmente para depurar.

TABLA 62 Propiedades del modo de inicio del host para servidores host SPARC *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI del SP:** `/HOST/bootmode`
- **Web del SP**: **Host Management (Gestión de host) > Host Boot Mode (Modo de inicio de host)**
- **Rol de usuario**: **Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades configurables del modo de inicio)**

Requisito:
- Para aplicar los cambios de las propiedades del modo de inicio en la página Host Boot Mode Settings (Configuración del modo de inicio del host), debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
LDOM Config (Configuración de LDOM) `(config=)`	Factory-default (Valores predeterminados de fábrica)	*Factory-default | Valid LDOM Config* Indique a Oracle ILOM la configuración de LDOM que debe utilizar cuando se vuelva a encender el servidor host SPARC: ■ Factory-default (Valores predeterminados de fábrica): la configuración inicial en la que la plataforma aparece como un único sistema que aloja sólo un sistema operativo. Use la configuración de fábrica en Oracle ILOM para poder volver a acceder a todos los recursos del sistema (CPU, memoria, E/S) que puedan haber sido asignados a otros dominios. El valor de la propiedad Factory-default (Valores predeterminados de fábrica) puede ser necesario si eliminó el gestor de dominios lógicos antes de restaurar los valores predeterminados de fábrica con el software Logical Domains del sistema operativo. ■ Valid LDOM Config (Configuración válida de LDOM): escriba el nombre de una configuración de dominios lógicos activa y válida. **Sintaxis de la CLI para la configuración de LDOM del modo de inicio del host**: **`set /HOST/bootmode`** **`config=`***factory-default|valid_LDOM_configuration*

Gestión de dominios de host SPARC

Oracle ILOM proporciona un conjunto de propiedades de dominio de host que permiten a los administradores del sistema ver las configuraciones de dominio lógico actuales del servidor host SPARC, así como las propiedades de dominio de host para el inicio automático y el inicio de invitados.

Las propiedades de dominio de host de Oracle ILOM se pueden ver y configurar desde la CLI y la interfaz web de Oracle ILOM. Si desea obtener información detallada sobre estas propiedades, consulte las siguientes tablas:

- Tabla 63
- Tabla 64

TABLA 63 Visualización de las configuraciones de dominio lógico detectadas para servidores host SPARC

Destino configurable de la interfaz de usuario:
- **CLI del SP:** `/HOST/domain/configs`
- **Web:** Host Management (Gestión de host) > Host Domain (Dominio de host)

Requisitos:
- Las configuraciones de los dominios lógicos se deben crear en el sistema operativo del servidor host SPARC. Si desea obtener información para crear configuraciones de dominio lógico, consulte la documentación de Oracle VM Server para SPARC.
- Para ver las configuraciones de dominio lógico, ejecute el comando show (`show /HOST/domain/configs`).

Propiedad	Descripción
Domain Configurations (read-only) (Configuraciones de dominio [sólo lectura])	Oracle ILOM muestra una lista de las configuraciones de dominio lógico detectadas en el sistema operativo host. Oracle guarda las configuraciones de dominio lógico detectadas en la memoria no volátil y actualiza la lista cuando se producen cambios.

TABLA 64 Propiedades configurables del dominio del host para servidores host SPARC

Destino configurable de la interfaz de usuario:

- **CLI del SP:** `/HOST/domain/control`
- **Web**: Host Management (Gestión de host) > Host Domain (Dominio de host)
- **Rol de usuario**: Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar las propiedades configurables del dominio del host)

Requisitos:

- Las configuraciones de los dominios lógicos se deben crear en el sistema operativo del servidor host SPARC. Si desea obtener información para crear configuraciones de dominio lógico, consulte la documentación de Oracle VM Server para SPARC.
- Para aplicar los cambios de las propiedades de dominio del host en la página Host Domain Settings (Configuración del dominio del host), debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Auto-Run (Ejecución automática) (`auto-boot=`)	Enabled (Activado)	*Enabled* |*Disabled* Cuando está activada la propiedad Auto-Run (Ejecución automática), Oracle ILOM reinicia automáticamente el dominio de control después del siguiente encendido o restablecimiento. Si la propiedad Auto-Run (Ejecución automática) está desactivada, se impide el inicio automático y el dominio de control del host se detiene en el indicador de estado de OpenBoot en el siguiente encendido o restablecimiento del servidor. **Sintaxis de la CLI para la ejecución automática del dominio del host**: **`set /HOST/domain/control auto-boot=`***enabled*|*disabled*
Boot Guests (Iniciar invitados) (`boot_guests=`)	Enabled (Activado)	*Enabled* |*Disabled* Cuando está activada la propiedad Boot Guests (Iniciar invitados), Oracle ILOM inicia los dominios invitados después del siguiente encendido o restablecimiento del servidor. Si la propiedad Boot Guests (Iniciar invitados) está desactivada, se impide el inicio de los dominios invitados configurados en el siguiente encendido o restablecimiento del servidor. **Sintaxis de la CLI para el inicio de invitados del dominio del host**: **`set /HOST/domain/control boot_guests=`***enabled*|*disabled*

Configuración del estado del selector para hosts SPARC

Oracle ILOM proporciona la propiedad KeySwitch (Selector) que permite a los administradores del sistema configurar el estado del selector para el servidor host SPARC. La propiedad KeySwitch se puede configurar desde la CLI o la interfaz web de Oracle ILOM. Si desea obtener información detallada sobre los valores de la propiedad configurable KeySwitch, consulte la siguiente tabla.

TABLA 65 Valores de la propiedad del estado del selector para servidores host SPARC

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI del SP:** /SYS
- **Web:** Host Management (Gestión de host) > KeySwitch > (Selector) > KeySwitch > (Selector)
- **Rol de usuario:** Admin (Administrador) (a) (se requiere para modificar la propiedad KeySwitch)

Requisito:
- Para aplicar los cambios de la propiedad KeySwitch en la interfaz web, debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
Keyswitch (Selector) `(keyswitch_state=)`	Normal	*Normal* |*Standby* |*Diag*|*Locked* ■ Normal: el servidor SPARC se puede encender automáticamente e iniciar el proceso de inicio. ■ Standby (En espera): el servidor SPARC no se enciende. ■ Diag (Diagnóstico): el servidor SPARC se puede encender automáticamente y utilizar los valores predeterminados de las propiedades de diagnóstico del host de Oracle ILOM para proporcionar cobertura de fallos. Si está activada, esta opción anula los valores de las propiedades de diagnóstico de Oracle ILOM especificados por el usuario. ■ Locked (Bloqueado): el servidor SPARC se puede encender automáticamente, pero está prohibida la actualización de los dispositivos Flash y la modificación del valor de la propiedad de la CLI configurado para `/HOST send_break_action=break`. **Sintaxis de la CLI para el selector**: **`set /SYS keyswtich_state=`***normal*|*standby*|*diag*|*locked*

Configuración del estado del módulo de plataforma de confianza para hosts SPARC

Oracle ILOM proporciona un conjunto de propiedades TPM de Oracle Solaris que permiten a los administradores del sistema gestionar el estado de la función de módulo de plataforma de confianza (TPM) en el servidor host SPARC. La propiedad TPM se puede configurar desde la CLI o la interfaz web de Oracle ILOM. Si desea obtener información detallada sobre los valores de la propiedad configurable TPM, consulte la siguiente tabla.

Nota – Las propiedades TPM de los servidores x86 se gestionan en la utilidad BIOS. Si desea obtener información detallada sobre las propiedades y los requisitos de TPM en sistemas operativos x86, consulte la guía de administración de servidores x86 de Oracle.

TABLA 66 Valores de la propiedad TPM para servidores host SPARC

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** `/HOST/tpm`
- **Web**: Host Management (Gestión de host) > TPM > TPM Settings > (Configuración de TPM)
- **Rol de usuario**: Reset and Host Control (Restablecimiento y control del host) (r) (se requiere para modificar la propiedad TPM)

Requisitos:

- El servidor host SPARC debe estar ejecutando una versión del sistema operativo de Oracle Solaris que admita TPM.
- Para aplicar las modificaciones de la propiedad de TPM en la interfaz web, debe hacer clic en Save (Guardar).

Propiedad	Valor predeterminado	Descripción
TPM (`activate= enable= forceclear=`)	Disabled (Desactivada)	*Active* | *Enable* |*Forceclear* ■ Enable (TPM state) (Activar [estado de TPM]): esta opción se debe activar (configurar con el valor true]) en Oracle ILOM para aplicar las modificaciones de la configuración de TPM. ■ Activate (Habilitar): esta opción y la opción Enable (Activar) se deben activar (configurar con el valor true) en Oracle ILOM para habilitar la configuración de TPM. ■ Forceclear (Forzar borrado): esta opción y la opción Enable (Activar) deben estar desactivadas (configuradas con el valor false) para purgar el estado de TPM en el siguiente restablecimiento. **Sintaxis de la CLI para el selector**: **`set /tpm activate=`***false*|*true* **`enable=`***false*|*clear* **`forceclear=`***false*|*enable*

Configuración de las notificaciones de alerta y el servidor Syslog para el registro de eventos

Descripción	Vínculos
Consulte esta sección para obtener información sobre cómo configurar, probar y desactivar las notificaciones de alerta.	■ "Configuración de las notificaciones de alerta" en la página 177
Consulte esta sección para obtener información sobre cómo configurar el servidor Syslog para registrar los eventos de Oracle ILOM en un host remoto.	■ "Configuración de Syslog para el registro de eventos" en la página 183

Información relacionada

- *User?s Guide*, Managing Oracle ILOM Log Entries
- *SNMP, IPMI, CIM, WS-MAN Protocol Management*, Managing SNMP Trap Alerts Using the Oracle ILOM
- Tabla 37

Configuración de las notificaciones de alerta

Los administradores del sistema pueden configurar notificaciones de alerta en Oracle ILOM para advertir con antelación sobre posibles fallos del sistema. Oracle ILOM admite la configuración de alertas PET de IPMI, alertas de capturas de SNMP y notificaciones de alerta por correo electrónico.

Es posible configurar hasta 15 notificaciones de alerta en Oracle ILOM con la CLI o la interfaz web de Oracle ILOM, o con un cliente SNMP. Para cada notificación de alerta configurada, los administradores del sistema pueden generar, de manera opcional, un mensaje de prueba a fin de garantizar que el destinatario reciba el mensaje de prueba correctamente.

Para obtener más información sobre cómo configurar notificaciones de alerta en Oracle ILOM, consulte los temas siguientes:

- "Propiedades de configuración de las notificaciones de alerta" en la página 178
- "Configuración y prueba de las notificaciones de alerta (PET de IPMI, SNMP o correo electrónico)" en la página 180

- "Desactivación de las notificaciones de alerta (PET de IPMI, SNMP o correo electrónico)" en la página 182
- "Configuración del cliente SMTP para alertas por correo electrónico" en la página 182

Propiedades de configuración de las notificaciones de alerta

Para cada notificación de alerta, es necesario definir estas tres propiedades en Oracle ILOM: `alert type`, `alert destination` y `alert level`. Según qué tipo de alerta se configure, será posible configurar otras propiedades opcionales.

Consulte la siguiente tabla para obtener más detalles sobre las propiedades de configuración de las notificaciones de alerta.

TABLA 67 Propiedades de configuración de las notificaciones de alerta

Propiedad	Requisito	Descripción
Alert Type (Tipo de alerta)	Obligatorio	La propiedad Alert Type indica el formato del mensaje y el método de entrega que Oracle ILOM utilizará al crear y enviar el mensaje de alerta. Las opciones de tipo de alerta incluyen: ▪ **IPMI PET Alerts** (Alertas PET de IPMI). Las propiedades obligatorias son: dirección IP de destino de la alerta y nivel de alerta. Cada destino especificado de la alerta debe admitir la recepción de mensajes PET de IPMI. ▪ **SNMP Trap Alerts** (Alertas de capturas de SNMP). Las propiedades obligatorias son: dirección IP de destino de la alerta, número de puerto de destino de la alerta y nivel de alerta. Cada destino especificado debe admitir la recepción de mensajes de capturas de SNMP. ▪ **Email Alerts** (Alertas por correo electrónico). Las propiedades obligatorias son: dirección de correo electrónico de destino y nivel de alerta. Antes de activar las alertas por correo electrónico, se deben configurar las propiedades del servidor de correo SMTP en Oracle. ILOM. **Información relacionada**: ▪ *SNMP, IPMI, CIM, WS-MAN Protocol Management*, Configuring SMTP Client for Email Alert Notifications (SNMP)
Alert Destination (Destino de alerta)	Obligatorio	La propiedad Alert Destination especifica dónde se enviará el mensaje de alerta. Los destinos de dirección IP se deben configurar para las alertas PET de IPMI y SNMP. Los destinos de dirección de correo electrónico se deben configurar para las alertas por correo electrónico.

TABLA 67 Propiedades de configuración de las notificaciones de alerta *(Continuación)*

Propiedad	Requisito	Descripción
Alert Destination Port (Puerto de destino de alerta)	Opcional	El puerto de destino TCP/UDP sólo se aplica a las configuraciones de alertas SNMP. Oracle ILOM selecciona automáticamente un número de puerto de destino TCP/UDP estándar. Los administradores del sistema pueden optar por aceptar el número de puerto estándar (162) o especificar un número de puerto TCP/UDP manualmente.
Alert Level (Nivel de alerta)	Obligatorio	Es necesario definir un nivel de alerta en todas configuraciones de notificaciones de alerta. Los niveles de alerta permiten enviar la notificación de alerta. Asimismo, para las alertas PET de IPMI y las alertas por correo electrónico, los niveles de alerta actúan como un mecanismo de filtro para garantizar que los destinatarios de la alerta sólo reciban los mensajes de alerta que más les interesan. Oracle ILOM ofrece los siguientes niveles de alerta, de los cuales Minor (Secundario) es el más bajo: ■ **Minor** (Secundario): genera alertas para eventos de tipo informativo, además de eventos principales y críticos. ■ **Major** (Principal): genera alertas para todos los eventos no críticos, irrecuperables y críticos. ■ **Critical** (Crítico): genera alertas para todos los eventos críticos e irrecuperables. ■ **Disabled** (Desactivado): desactiva la configuración de alertas. Oracle ILOM no generará ningún mensaje de alerta. **Importante**: Oracle ILOM admite el filtro de niveles de alerta para todas las configuraciones de alertas PET de IPMI y las configuraciones de alertas por correo electrónico. Oracle ILOM no admite el filtro de niveles de alerta para las configuraciones de alertas SNMP. Sin embargo, para activar Oracle ILOM a fin de generar una alerta SNMP, se debe especificar uno de los siguientes niveles de alerta: *Minor* (Secundario), *Major* (Principal) o *Critical* (Crítico).
Email Custom Sender (Remitente personalizado de correo electrónico)	Opcional para alertas por correo electrónico	De manera opcional, los administradores del sistema pueden configurar esta propiedad sólo para las configuraciones de alertas por correo electrónico. La propiedad email_custom_sender permite a Oracle ILOM sustituir la dirección del remitente del cliente SMTP mediante una de las siguientes cadenas: <*IPADDRESS*> o <*HOSTNAME*>. **Ejemplo:** alert@<*IPADDRESS*>.
Email Message Prefix (Prefijo de mensaje de correo electrónico)	Opcional para alertas por correo electrónico	De manera opcional, los administradores del sistema pueden configurar esta propiedad sólo para las configuraciones de alertas por correo electrónico. La propiedad Email Message Prefix permite a Oracle ILOM anteponer información especificada por el usuario al cuerpo del mensaje.

TABLA 67 Propiedades de configuración de las notificaciones de alerta *(Continuación)*

Propiedad	Requisito	Descripción
Event Class Filter (Filtro de clases de evento)	Opcional para alertas por correo electrónico	De manera opcional, los administradores del sistema pueden configurar esta propiedad sólo para las configuraciones de alertas por correo electrónico. La propiedad Event Class Filter permite a Oracle ILOM filtrar toda la información, excepto la clase de evento seleccionada. Para borrar el filtro y enviar información sobre todas las clases, utilice comillas dobles vacías ("“).
Event Type Filter (Filtro de tipos de evento)	Opcional para alertas por correo electrónico	De manera opcional, los administradores del sistema pueden configurar esta propiedad sólo para las configuraciones de alertas por correo electrónico. La propiedad Event Type Filter permite a Oracle ILOM filtrar toda la información, excepto el tipo de evento seleccionado. Para borrar el filtro y enviar información sobre todos los tipos de evento, utilice comillas dobles vacías ("“).
SNMP Version (Versión de SNMP)	Opcional para alertas SNMP	La propiedad SNMP Version permite a los administradores del sistema especificar la versión de captura de SNMP que se enviará. Las versiones admitidas de SNMP son: 1, 2c o 3.
SNMP Community Name (Nombre de comunidad SNMP) o User Name (Nombre de usuario)	Opcional para alertas SNMP	De manera opcional, los administradores del sistema pueden especificar una cadena de comunidad SNMPv1 o 2c o un nombre de usuario SNMPv3. **Nota –** Si se configura un nombre de usuario SNMPv3, el nombre de usuario SNMPv3 se deberá configurar en Oracle ILOM. Si no se configura el nombre de usuario SNMP, la alerta no se autenticará para el envío.

▼ Configuración y prueba de las notificaciones de alerta (PET de IPMI, SNMP o correo electrónico)

En el siguiente procedimiento, se proporcionan instrucciones para configurar y probar las notificaciones de alerta con la CLI y la interfaz web de Oracle ILOM. Si desea obtener instrucciones para configurar y probar las notificaciones de alerta desde un cliente de aplicación SNMP, consulte el .

Antes de empezar

- Para las configuraciones de alertas por correo electrónico, se debe configurar el servidor SMTP. Si no se configura el servidor SMTP, Oracle ILOM no podrá generar alertas por correo electrónico. Para obtener detalles sobre la configuración, consulte "Configuración del cliente SMTP para alertas por correo electrónico" en la página 182.

- Para las configuraciones de alertas SNMP, se debe activar la propiedad para SNMP sets y se debe configurar al menos una cuenta de usuario para SNMP. Para obtener detalles sobre la configuración, consulte Tabla 37.
- Se requiere el rol Admin (a) en Oracle ILOM para configurar las propiedades de las notificaciones de alerta.

1 Para completar las propiedades de uno de los 15 ID de configuración de alertas, haga lo siguiente:

- **Web:**

  Haga clic en ILOM Administration (Administración de ILOM) > Notifications (Notificaciones) > Alerts (Alertas) y, a continuación, haga clic en un ID de alerta y en Edit (Editar). Defina las propiedades obligatorias (nivel, tipo y destino) y haga clic en Save (Guardar).

  Para obtener detalles sobre las propiedades obligatorias y opcionales, consulte Tabla 67.

- **CLI:**

  Escriba lo siguiente para definir las propiedades obligatorias de las alertas:

  set /*SP*|*CMM***/alertmgmt/rules/***n* **type=***email*|*snmptrap*|*ipmipet* **destination=***ip_address* **port=***required_for_snmptrap* **level=***minor*|*major*|*critical*|*disable*

  Para obtener detalles sobre las propiedades obligatorias y opcionales, consulte Tabla 67.

2 Para probar la configuración de una notificación de alerta, haga lo siguiente:

- **Web:**

  Haga clic en ILOM Administration (Administración de ILOM) > Notifications (Notificaciones) > Alerts (Alertas) y, a continuación, haga clic en un ID de alerta configurado y en Test Rule (Probar regla).

  Aparece un mensaje de estado correcto o con errores.

- **CLI:**

  Escriba lo siguiente para probar una notificación de alerta configurada:

  set /*SP*|*CMM***/alertmgmt/rules/***n* **testalert=true**

  Aparece un mensaje de estado correcto o con errores.

Más información

Información relacionada:

- Tabla 67
- “Configuración del cliente SMTP para alertas por correo electrónico” en la página 182

- Tabla 37
- *User?s Guide*, Managing Oracle ILOM Log Entries
- *SNMP, IPMI, CIM, WS-MAN Protocol Management*, Managing SNMP Trap Alerts Using the Oracle ILOM

▼ Desactivación de las notificaciones de alerta (PET de IPMI, SNMP o correo electrónico)

En el siguiente procedimiento, se proporcionan instrucciones para desactivar una notificación de alerta configurada con la CLI y la interfaz web de Oracle ILOM. Si desea obtener instrucciones para desactivar una notificación de alerta configurada desde un cliente de aplicación SNMP, consulte el .

Antes de empezar

- Se requiere el rol Admin (a) en Oracle ILOM para modificar las propiedades de las notificaciones de alerta.

● **Para desactivar la configuración de una notificación de alerta, haga lo siguiente:**

- **Web:**

  Haga clic en ILOM Administration (Administración de ILOM) > Notifications (Notificaciones) > Alerts (Alertas) y, a continuación, haga clic en un ID de alerta configurado y en Edit (Editar). En el cuadro de lista Level (Nivel), haga clic en Disable (Desactivar) y en Save (Guardar).

  Aparece un mensaje de estado correcto o con errores.

- **CLI:**

  Escriba lo siguiente para desactivar una notificación de alerta configurada:

  set /*SP|CMM***/alertmgmt/rules/***n* **level=disable**

  Aparece un mensaje de estado correcto o con errores.

▼ Configuración del cliente SMTP para alertas por correo electrónico

En el siguiente procedimiento, se describe cómo configurar Oracle ILOM como cliente SMTP con la CLI o la interfaz web de Oracle ILOM. Oracle ILOM debe actuar como cliente SMTP para enviar notificaciones de alerta por correo electrónico correctamente.

Antes de empezar

- Antes de configurar Oracle ILOM como cliente SMTP, determine la dirección IP y el número de puerto del servidor de correo SMTP saliente que procesará las notificaciones por correo electrónico.
- La propiedad SMTP Client (Cliente de SMTP) para Custom Sender (Remitente personalizado) es opcional. Esta propiedad permite a Oracle ILOM sustituir la dirección del remitente SMTP mediante una de las siguientes cadenas: <*IPADDRESS*> o <*HOSTNAME*>. Por ejemplo: alert@[*IPADDRESS*]
- Se requiere el rol Admin (a) en Oracle ILOM para configurar las propiedades del cliente SMTP.

● **Para configurar Oracle ILOM como cliente SMTP, haga lo siguiente:**

- **Web:**

  Haga clic en ILOM Administration (Administración de ILOM) > Notifications (Notificaciones) > SMTP Client (Cliente SMTP).

  Active el estado de SMTP, complete las propiedades obligatorias para la dirección IP y el número de puerto del servidor SMTP, complete la propiedad opcional para Custom Sender (Remitente personalizado), si es necesario, y haga clic en Save (Guardar).

- **CLI:**

  Escriba:

  set /*SP*|*CMM***/clients/smtp state=enable address=***smtp_server_ip*
  port=*smtp_server_port* **custom_send=***optional_string*

Más información

Información relacionada:

- "Configuración y prueba de las notificaciones de alerta (PET de IPMI, SNMP o correo electrónico)" en la página 180

Configuración de Syslog para el registro de eventos

Syslog es un servicio de protocolo utilizado para registrar eventos en un host de registro remoto. Los administradores del sistema pueden activar el servicio Syslog en Oracle ILOM mediante la configuración de la dirección IP de un servidor Syslog.

Los eventos registrados en un servidor Syslog proporcionan la misma información que se muestra en el registro de eventos local de Oracle ILOM, como clase, tipo, gravedad y descripción. Oracle ILOM incluye propiedades para configurar hasta dos servidores Syslog.

Configuración de la dirección IP de Syslog para el registro de eventos

Antes de empezar

- Se requiere el rol Admin (a) en Oracle ILOM para modificar las propiedades de Syslog.

● **Para completar la dirección IP en una de las dos propiedades de Syslog, haga lo siguiente:**

- **Web:**

  Haga clic en ILOM Administration (Administración de ILOM) > Notifications (Notificaciones) > Syslog.

  Escriba la dirección IP del servidor Syslog en el cuadro de texto Server 1 (Servidor 1) o Server 2 (Servidor 2), y haga clic en Save (Guardar).

- **CLI:**

  Escriba:

  set /*SP*|*CMM***/clients/syslog destination_ip=***syslog_server_ip*

Más información

Información relacionada:

- *User?s Guide*, Managing Oracle ILOM Log Entries

Configuración de políticas de gestión del sistema

Descripción	Vínculos
Consulte esta sección para obtener descripciones de las políticas de gestión del sistema que es posible configurar desde el SP del servidor.	■ “Políticas de gestión del sistema configurables desde el SP del servidor” en la página 185
Consulte esta sección para obtener descripciones de las políticas de gestión del sistema que es posible configurar desde el CMM.	■ “Políticas de gestión del sistema configurables desde el CMM” en la página 187

Información relacionada

- “Configuración de notificaciones de alerta de energía y gestión del uso de energía del sistema” en la página 191

Políticas de gestión del sistema configurables desde el SP del servidor

De manera opcional, los administradores del sistema pueden definir políticas de gestión del sistema desde el SP del servidor para controlar las políticas de encendido y apagado en el inicio, así como las políticas de refrigeración para los componentes del sistema.

De forma predeterminada, todas las políticas de gestión del sistema están desactivadas en el SP de Oracle ILOM. Consulte la siguiente tabla para obtener descripciones sobre las propiedades de las políticas de gestión del sistema que es posible configurar desde el SP del servidor.

TABLA 68 Políticas de gestión del sistema del SP del servidor

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** */SP/policy*
- **Web:** **System Management (Gestión del sistema) > Policy (Política) > Policy Configuration (Configuración de política)**
- **Rol de usuario:** **admin (a) (requerido para todas las modificaciones de propiedades)**

Política de gestión del sistema	Descripción
Auto-Power-On Host on Boot (Encender automáticamente el host al iniciar) (`HOST_AUTO_POWER_ON=`)	*Disabled* (predeterminado)|*Enabled* Active esta política para encender automáticamente el sistema operativo del servidor host al iniciar. **Nota –** Al activar esta política, se desactiva automáticamente la política “Configurar host en último estado de energía al iniciar” si está activada. **Sintaxis de la CLI para encender automáticamente el host al iniciar** **`Set /SP/policy HOST_AUTO_POWER_ON=`***enabled*|*disabled*
Set Host to Last Power State on Boot (Configurar host en último estado de energía al iniciar) (`HOST_LAST_POWER_STATE=`)	*Disabled* (predeterminado)|*Enabled* Active esta política para configurar el estado de energía del servidor host en el último estado conocido al iniciar. **Nota –** Al activar esta política, se desactiva automáticamente la política “Encender automáticamente el host al iniciar” si está activada. **Sintaxis de la CLI para configurar host en último estado de energía al iniciar** **`Set /SP/policy HOST_LAST_POWER_STATE=`***enabled*|*disabled*
Set to Delay Host Power On (Configurar retraso de encendido del host) (servidor SPARC únicamente) (`HOST_AUTO_POWER_ON=`)	*Disabled* (predeterminado)|*Enabled* Active esta política en un servidor SPARC de Oracle para retrasar el encendido del sistema operativo del host al iniciar. **Sintaxis de la CLI para configurar retraso de encendido** **`Set /SP/policy HOST_AUTO_POWER_ON=`***enabled*|*disabled*

TABLA 68 Políticas de gestión del sistema del SP del servidor *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** */SP/policy*
- **Web:** **System Management (Gestión del sistema) > Policy (Política) > Policy Configuration (Configuración de política)**
- **Rol de usuario:** **admin (a) (requerido para todas las modificaciones de propiedades)**

Política de gestión del sistema	Descripción
Set Enhanced PCIe Cooling Mode (Configurar modo de refrigeración de PCIe mejorado) (servidor x86 únicamente) (`ENHANCED_PCIE_COOLING_MODE=`)	*Disabled* (predeterminado)|*Enabled* Active esta política en un servidor x86 de Oracle para satisfacer los requisitos de temperatura de funcionamiento del refrigerador para determinadas tarjetas PCIe de un servidor x86. El modo de política de refrigeración de PCIe, cuando está activado, indica a Oracle ILOM que disminuya los umbrales del sensor de temperatura de salida del chasis utilizados por el algoritmo del ventilador del chasis para mantener el funcionamiento de las tarjetas PCIe dentro del rango de temperatura requerido. **Sintaxis de la CLI para configurar modo de refrigeración de PCIe mejorado** **`Set /SP/policy ENHANCED_PCIE_COOLING_MODE=`***enabled*|*disabled*
Enable a Cooldown Period Before Host Shuts Down (Permitir período de refrigeración antes de apagar el host) (`HOST_AUTO_POWER_ON=`)	*Disabled* (predeterminado)|*Enabled* Active esta propiedad en los servidores SPARC para acceder a un modo de refrigeración al apagar el servidor host. El modo de refrigeración indica a Oracle ILOM que supervise determinados componentes para asegurarse de que estén por debajo de una temperatura mínima para no provocar daños al usuario. Una vez que los subcomponentes del servidor están por debajo de la temperatura mínima, se desactivará la energía del servidor o se apagará el host si el proceso tarda más de cuatro minutos en completarse. **Sintaxis de la CLI para permitir período de refrigeración antes de apagar el host** **`Set /SP/policy HOST_AUTO_POWER_ON=`***enabled*|*disabled*

Políticas de gestión del sistema configurables desde el CMM

De manera opcional, los administradores del sistema pueden definir políticas de gestión del sistema desde el CMM para gestionar la demanda de las fuentes de alimentación del chasis, las velocidades del ventilador de las fuentes de alimentación, la función SAS-2 del blade de almacenamiento y la gestión de energía del chasis.

Consulte la siguiente tabla para obtener descripciones sobre las propiedades de las políticas de gestión del sistema que es posible configurar desde el CMM.

TABLA 69 Política de gestión del servidor del CMM

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** `/CMM/policy` -o- `/CH/BLn/SP/policy`
- **Web:** System Management (Gestión del sistema) > Policy (Política) > Policy Configuration (Configuración de política)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Política de gestión del sistema	Valor predeterminado	Descripción
Light Load Efficiency Mode (Modo de eficiencia de carga de luz) (`LIGHT_LOAD_EFFICIENCY_MODE=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Active esta política para supervisar la energía que utiliza el sistema del chasis y apagar automáticamente los lados de la unidad de fuente de alimentación (PSU) para lograr una mayor eficiencia. **Sintaxis de la CLI para modo de eficiencia de carga de luz** **`Set /CMM/policy LIGHT_LOAD_EFFICIENCY_MODE=`***enabled*|*disabled*
Monitor Power Supply 0 Side 0 for power (Supervisar fuente de alimentación 0 lado 0 para energía) (`MONITOR_PS0_SIDE0=`)	Enabled (Activado)	*Disabled* |*Enabled* Active esta política para permitir la supervisión de la fuente de alimentación 0 lado 0 en el modo de eficiencia de carga de luz. **Sintaxis de la CLI para supervisar fuente de alimentación 0 lado 0** **`Set /CMM/policy MONITOR_PS0_SIDE0=`***enabled*|*disabled*
Monitor Power Supply 0 Side 1 for power (Supervisar fuente de alimentación 0 lado 1 para energía) (`MONITOR_PS0_SIDE1=`)	Enabled (Activado)	*Disabled* |*Enabled* Active esta política para permitir la supervisión de la fuente de alimentación 0 lado 1 en el modo de eficiencia de carga de luz. **Sintaxis de la CLI para supervisar fuente de alimentación 0 lado 1** **`Set /CMM/policy MONITOR_PS0_SIDE1=`***enabled*|*disabled*
Monitor Power Supply 1 Side 0 for power (Supervisar fuente de alimentación 1 lado 0 para energía) (`MONITOR_PS1_SIDE0=`)	Enabled (Activado)	*Disabled* |*Enabled* Active esta política para permitir la supervisión de la fuente de alimentación 1 lado 0 en el modo de eficiencia de carga de luz. **Sintaxis de la CLI para supervisar fuente de alimentación 1 lado 0** **`Set /CMM/policy MONITOR_PS1_SIDE0=`***enabled*|*disabled*

TABLA 69 Política de gestión del servidor del CMM *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI:** `/CMM/policy` *-o-* `/CH/BLn/SP/policy`
- **Web:** System Management (Gestión del sistema) > Policy (Política) > Policy Configuration (Configuración de política)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Política de gestión del sistema	Valor predeterminado	Descripción
Monitor Power Supply 1 Side 1 for power (Supervisar fuente de alimentación 1 lado 1 para energía) (`MONITOR_PS1_SIDE1=`)	Enabled (Activado)	*Disabled* |*Enabled* Active esta política para permitir la supervisión de la fuente de alimentación 1 lado 1 en el modo de eficiencia de carga de luz. **Sintaxis de la CLI para supervisar fuente de alimentación 1 lado 1** **`Set /CMM/policy MONITOR_PS1_SIDE1=`***enabled*|*disabled*
Sun Cooling Door Installed (Puerta de refrigeración Sun instalada) (`COOLING_DOOR_INSTALLED=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Active esta política para admitir la instalación de una puerta de refrigeración en un chasis Sun Blade 6048. **Sintaxis de la CLI para puerta de refrigeración instalada** **`Set /CMM/policy COOLING_DOOR_INSTALLED=`***enabled*|*disabled*
Force Power Supply Fans to High Speed (Forzar ventiladores de fuente de alimentación en velocidad alta) (`PS_FANS_HIGH=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Active esta política para forzar los ventiladores de la fuente de alimentación a funcionar al 100% de su capacidad. **Sintaxis de la CLI para forzar ventiladores de fuente de alimentación en velocidad alta** **`Set /CMM/policy PS_FANS_HIGH=`***enabled*|*disabled*
Force Power Supply Fans to Low Speed (Forzar ventiladores de fuente de alimentación en velocidad baja) (`PS_FANS_LOW=`)	Disabled (Desactivado)	*Disabled* |*Enabled* Active esta política para forzar los ventiladores de la fuente de alimentación a funcionar al 80% de su capacidad. **Sintaxis de la CLI para forzar ventiladores de fuente de alimentación en velocidad baja** **`Set /CMM/policy PS_FANS_LOW=`***enabled*|*disabled*

TABLA 69 Política de gestión del servidor del CMM *(Continuación)*

Destino y rol de usuario configurables de la interfaz de usuario:
- **CLI:** `/CMM/policy` *-o-* `/CH/BLn/SP/policy`
- **Web:** System Management (Gestión del sistema) > Policy (Política) > Policy Configuration (Configuración de política)
- **Rol de usuario:** admin (a) (requerido para todas las modificaciones de propiedades)

Política de gestión del sistema	Valor predeterminado	Descripción
Force Server Blade to be SAS2 Capable at 3Gbps (Forzar compatibilidad de servidor blade con SAS2 en 3 Gbps) `(BLn_FORCE_SAS2_3GBPS= disabled)`	Disabled (Desactivado)	*Disabled |Enabled* Active esta política para forzar los NEM a ejecutar el vínculo SAS a una velocidad inferior, en el caso poco probable de que esta acción sea necesaria. **Sintaxis de la CLI para forzar compatibilidad de servidor blade con SAS2 en 3 Gbps** **`Set /CH/BLn/SP/policy PS_FANS_LOW=`***enabled|disabled*
Manage Chassis Power. Warning: Disabling May Lead to Chassis Shutdown (Gestionar energía del chasis. Advertencia: Si se desactiva, es posible que el chasis se apague) `(POWER_MANAGEMENT=)`	Enabled (Activado)	*Disabled |Enabled* Active esta política para determinar si hay suficiente energía en el chasis para encender un nuevo módulo de servidor instalado en el chasis. **Sintaxis de la CLI para gestionar energía del chasis. Advertencia: Si se desactiva, es posible que el chasis se apague** **`Set /CMM/policy POWER_MANAGEMENT=`***enabled|disabled*

Configuración de notificaciones de alerta de energía y gestión del uso de energía del sistema

Descripción	Vínculos
Consulte esta sección para obtener descripciones de las propiedades configurables de CMM y SP para notificaciones de alerta de consumo de energía.	■ "Configuración de notificaciones de alerta de consumo de energía" en la página 192
Consulte estas secciones para obtener descripciones de las propiedades configurables de CMM y SP para la gestión del uso de energía del sistema.	■ "Configuración de las propiedades de límite de energía del SP y de otorgamiento de energía del CMM" en la página 193 ■ "Definición de la política avanzada de limitación de energía del SP para aplicar el límite de energía" en la página 196 ■ "Configuración de la política de redundancia de la fuente de alimentación del CMM" en la página 198

Información relacionada

- *User?s Guide*, Real-Time Power Monitoring Through Oracle ILOM Interfaces
- *SNMP, IPMI, CIM, WS-MAN Protocol Management*, Manage SPARC Diagnostics, POST, and Boot Mode Operations (SNMP)
- "Configuración de las notificaciones de alerta y el servidor Syslog para el registro de eventos" en la página 177

Configuración de notificaciones de alerta de consumo de energía

Oracle ILOM ofrece propiedades de configuración para dos notificaciones de consumo de energía. Cuando están activadas, los destinatarios de correo electrónico configurados reciben notificaciones de alerta cuando la energía del sistema supera los umbrales establecidos.

Los umbrales de consumo de energía y las notificaciones de alerta por correo electrónico se pueden configurar desde la interfaz web o la CLI de Oracle ILOM.

Para obtener información detallada sobre cómo configurar una notificación de alerta por correo electrónico, consulte "Configuración de las notificaciones de alerta" en la página 177.

Para obtener información detallada sobre las propiedades de configuración para los umbrales de notificación de energía, consulte la tabla siguiente.

TABLA 70 Propiedades de configuración de los umbrales de notificación de consumo de energía

Destino y rol de usuario configurables de la interfaz de usuario:

- **CLI del SP:** /SP|CMM /powermgmt
- **Web:** Power Management (Gestión de energía) > Consumption (Consumo) > Notification Threshold 1 | 2 (Umbral de notificación 1 | 2)
- El rol Admin (a) (necesario para modificar las propiedades del umbral).

Requisitos:

- Para aplicar modificaciones a las propiedades del umbral en la interfaz web, debe hacer clic en Save (Guardar).
- Las propiedades de notificación de alertas por correo electrónico se deben configurar en Oracle ILOM.

Propiedad	Valor predeterminado	Descripción
Umbral de notificación 1 y 2 (threshold1=*n* |threshold2=*n*)	Disabled (Desactivado)	*Disabled (Desactivado) | Enabled (Activado)* ■ Disabled (Desactivado): cuando está desactivado, el estado de propiedad del umbral de notificación y el valor de la propiedad de vataje (*0*) están desactivados. ■ Enabled (Activado): cuando está activado, el estado de propiedad del umbral de notificación y el valor de la propiedad de vataje especificado por el usuario se pueden configurar. Especifique un valor de umbral de vataje entre 1 y 65535. Oracle ILOM genera un evento de alerta si la energía del sistema supera el umbral establecido. Si se configura un destinatario de alerta por correo electrónico, Oracle ILOM también genera un alerta por correo electrónico del consumo de energía al destinatario configurado. **Sintaxis de la CLI para el umbral de notificación de consumo de energía** **set /SP/CMM/powermgmt threshold1=***<0 to 65535>* **threshold2=***<0 to 65535>* **Información relacionada:** ■ “Configuración de las notificaciones de alerta” en la página 177

Configuración de las propiedades de límite de energía del SP y de otorgamiento de energía del CMM

Oracle ILOM cuenta con propiedades configurables de SP y CMM para limitar y otorgar el uso de energía en un sistema gestionado. Estas propiedades de limitación y otorgamiento de energía se pueden configurar desde la interfaz web y la CLI de Oracle ILOM a partir de la versión de firmware 3.1.1 o una posterior.

Para obtener más información sobre las propiedades configurables en Oracle ILOM para la limitación y el otorgamiento de energía, consulte estos temas:

- “Definición de las propiedades de límite de destino de energía del SP” en la página 194

- "Definición de la propiedad del límite de otorgamiento a las ranuras del blade del CMM" en la página 195

Definición de las propiedades de límite de destino de energía del SP

Antes de empezar

- La versión de firmware 3.1.2 o posterior de SP de Oracle ILOM debe estar instalada en el servidor gestionado.
- Se requiere el rol Admin (a) en Oracle ILOM para modificar las propiedades de límite de energía.
- La opción Power Target Limit (Límite de destino de energía), cuando está activada, controla la cantidad de energía que el servidor gestionado puede consumir.

Este procedimiento proporciona instrucciones web y de la CLI del SP.

- **Para activar las propiedades de límite de destino de energía del SP, realice uno de los siguientes procedimientos en la interfaz de Oracle ILOM:**

Interfaz de Oracle ILOM	Procedimiento para definir el límite de destino de energía
Web	a. Haga clic en Power Management (Gestión de energía) > Power Limit (Límite de energía). b. Establezca un valor de límite de destino en vatios o un porcentaje. El límite de destino se debe establecer entre la energía mínima recibida por los componentes de hardware instalados y la energía máxima que el servidor gestionado puede consumir (máximo permitido). c. Active el estado de Power Limiting (Limitación de energía). El estado Power Limiting debe estar activado para que Oracle ILOM active la configuración de límite de energía de destino. d. Haga clic en Save (Guardar) para aplicar los cambios.
CLI	■ Escriba: **set /SP/powermgmt/budget pending_power_limit=***value* **pendingactivation_state=enabled commit_pending=true** Donde *value* es el valor de límite de destino en vataje o el valor de límite de destino en porcentaje. El límite de destino se debe establecer entre la energía mínima recibida por los componentes de hardware instalados y la energía máxima que el servidor gestionado puede consumir (máximo permitido).

Más información

Información relacionada

- *User?s Guide*, Monitoring Power Allocations

- "Definición de la política avanzada de limitación de energía del SP para aplicar el límite de energía" en la página 196

▼ Definición de la propiedad del límite de otorgamiento a las ranuras del blade del CMM

Antes de empezar

- Se requiere la versión de firmware 3.1.1 o posterior de CMM de Oracle ILOM.
- Se requiere el rol Admin (a) en Oracle ILOM para modificar la propiedad Blade Slot Grant Limit (Límite de otorgamiento a las ranuras del blade).
- La propiedad Blade Slot Grant Limit (Límite de otorgamiento a las ranuras del blade) controla la cantidad de energía que CMM permite consumir a un servidor blade de CPU. De manera predeterminada, el límite de otorgamiento a las ranuras del blade es de 1200 vatios (límite máximo de energía de las ranuras del blade).

  Los administradores del sistema pueden elegir aceptar el límite de otorgamiento a las ranuras del blade predeterminado (1200 vatios) o modificarlo. Sin embargo, la propiedad de límite de otorgamiento no debe establecerse en un valor inferior al vataje de energía de ranuras del blade ya otorgado por el CMM (energía otorgada). Al establecer Blade Slot Grant Limit en 0, se impide que el servidor blade de CPU instalado se encienda.

Nota – Los servidores blade de almacenamiento instalados ignoran el límite de otorgamiento a las ranuras del blade. Los servidores blade de almacenamiento se alimentan automáticamente.

Este procedimiento proporciona instrucciones web y de la CLI del CMM.

● **Para definir la propiedad de límite de otorgamiento a ranura de blade del CMM, realice uno de los siguientes procedimientos en la interfaz de Oracle ILOM:**

Interfaz de Oracle ILOM	Procedimiento para definir el límite de otorgamiento a las ranuras del blade del CMM
Web	a. Haga clic en Power Management (Gestión de energía) > Allocation (Asignación). b. En la tabla Power Grants (Otorgamientos de energía), haga clic en el botón de radio ubicado junto a un servidor blade de CPU y, a continuación, en Edit (Editar). **Nota.** Los servidores blade de almacenamiento se muestran en la tabla como "Ignored Auto-Powered blade" (Blade alimentado automáticamente ignorado). La propiedad Blade Slot Grant Limit (Límite de otorgamiento a las ranuras del blade) es ignorada para los servidores blade de almacenamiento. c. En el cuadro de diálogo Edit (Editar), active una de las siguientes opciones de Blade Slot Grant Limit (Límite de otorgamiento a las ranuras del blade): **Slot Maximum** (Máximo de ranura) (valor predeterminado, 1200 vatios): cuando está activada esta opción, el CMM puede otorgar hasta 1200 vatios de energía al servidor blade de CPU solicitante. O bien: **Custom** (Personalizado): cuando está activada esta opción, escriba un número para el vataje de energía permitido que el CMM puede otorgar a un servidor blade de CPU solicitante. La cantidad de vataje de energía no debe ser inferior a la cantidad de vataje de energía ya otorgada a la ranura de blade por el CMM (energía otorgada). La definición del vataje de energía en 0 impedirá que el servidor blade de CPU instalado se encienda. d. Haga clic en Save (guardar) para aplicar los cambios.
CLI	■ Escriba: **set /CMM/powermgmt/powerconf/bladeslots/BL***n* **grant_limit=***watts* *Donde:* **n**: escriba el número de ranura de blade de un servidor blade de CPU instalado. **watts** (vatios): escriba un número para el vataje de energía permitido que el CMM puede otorgar a un servidor blade de CPU solicitante. La cantidad de vataje de energía no debe ser inferior a la cantidad de vataje de energía ya otorgada a la ranura de blade por el CMM (energía otorgada). La definición del vataje de energía en 0 impedirá que el servidor blade de CPU instalado se encienda.

Más información

Información relacionada

- *User?s Guide*, Power Consumption Terminology and Properties
- *User?s Guide*, Monitoring Power Allocations
- Política de CMM para la gestión de energía del chasis, "Políticas de gestión del sistema configurables desde el CMM" en la página 187

Definición de la política avanzada de limitación de energía del SP para aplicar el límite de energía

Oracle ILOM proporciona las propiedades de la política de limitación de energía del SP para aplicar el límite de energía del sistema. Estas propiedades se pueden configurar desde la interfaz web y desde la CLI de Oracle ILOM a partir de la versión de firmware 3.1.1 o posterior.

Para obtener más información acerca de cómo configurar las propiedades de la política de limitación de energía en Oracle ILOM, consulte el procedimiento siguiente.

▼ Definición de la política avanzada de limitación de energía

Antes de empezar

- Se requiere la versión de firmware 3.1.2 o posterior de SP de Oracle ILOM.
- Se requiere el rol de Admin (a) en Oracle ILOM para modificar las propiedades de la política avanzada de energía.
- La opción Advanced Power Capping Policy (Política avanzada de limitación de energía) ayuda a aplicar el límite de energía de destino del sistema al permitir que los administradores del sistema definan limitaciones flexibles con infracciones y período de gracia, o definan limitaciones rígidas para mantener el consumo de energía máximo permitido dentro del límite de energía de destino.

Este procedimiento proporciona instrucciones web y de la CLI del SP.

● **Para definir la política de limitación de energía del SP, realice uno de los siguientes procedimientos en la interfaz de Oracle ILOM:**

Interfaz de Oracle ILOM	Procedimiento para definir la política avanzada de limitación de energía
Web	a. Haga clic en Power Management (Gestión de energía) > Power Limit (Límite de energía). b. Active una de las siguientes opciones de la política avanzada de limitación de energía: **Soft Cap** (Limitación flexible) (opción predeterminada): cuando esta opción está activada, la energía del sistema se limita sólo si el consumo de energía del sistema (energía real) supera el límite de energía de destino y el período de gracia configurado por el usuario (el valor predeterminado es de 10 segundos). Los administradores del sistema pueden elegir aceptar el período de gracia predeterminado de 10 segundos o modificarlo haciendo clic en la opción Custom (Personalizado) y especificando segundos aceptables para el período de gracia permisible (de 0 a 99999). O bien: **Hard Cap** (Limitación rígida): cuando esta opción está activada, el consumo de energía del sistema se limita para mantener la energía máxima permitida dentro del límite de energía de destino. c. Active una de las siguientes acciones de infracción de política: **None** (Ninguna) (opción predeterminada): cuando esta opción está activada, no se realiza ninguna acción cuando el consumo de energía del sistema infringe la política de energía. O bien: **Hard Power Off** (Apagado forzoso): cuando esta opción está activada, el sistema se apaga inmediatamente cuando el consumo de energía del sistema infringe la política de energía. d. Haga clic en Save (Guardar) para aplicar los cambios.

Interfaz de Oracle ILOM	Procedimiento para definir la política avanzada de limitación de energía
CLI	a. Para definir la política avanzada de limitación de energía, escriba: **`set /SP/powermgmt policy=`***performance*|*elastic*|*none* *Donde*: **performance (rendimiento)** (opción predeterminada, equivalente a Soft Cap en Web): cuando se establece, la energía del sistema se limita sólo si el consumo de energía del sistema (energía real) supera: 1) el límite de energía de destino y la propiedad `timelimit` configurable por el usuario (el valor predeterminado es 10 segundos). O bien: **elastic** (elástica) (equivalente a Hard Cap en Web): cuando se establece, el consumo de energía del sistema se limita para mantener la energía máxima permitida dentro del límite de energía de destino. **none** (ninguno): cuando se establece esta opción, la política de energía se desactiva en Oracle ILOM.
	b. Para definir los parámetros `timelimit` y `vilolation_actions` cuando la se define la propiedad Performance (Rendimiento) para la política de energía, escriba: **`set /SP/powermgmt/budget pendingtimelimit=`***seconds* **`pendingviolation_actions=`***none*|*hardpoweroff* **`commit_pending=true`** *Donde:* **`seconds`**: escriba la cantidad de segundos aceptables (de 0 a 99999) para el período de gracia (el valor predeterminado es 10 segundos). **`none|hardpoweroff`** : escriba `none` para que el sistema no realice ninguna acción si se infringe la política de energía. Escriba `hardpoweroff` para pagar de inmediato el sistema si el consumo de energía del sistema infringe la política de energía.

Más información

Información relacionada

- *User?s Guide*, Power Consumption Terminology and Properties
- *User?s Guide*, Monitoring Power Allocations
- Política de CMM para la gestión de energía del chasis, "Políticas de gestión del sistema configurables desde el CMM" en la página 187

Configuración de la política de redundancia de la fuente de alimentación del CMM

Oracle ILOM proporciona una política de redundancia de la fuente de alimentación del CMM para impedir la pérdida de energía suministrada a los componentes de chasis del sistema blade. La política de redundancia de la fuente de alimentación se puede configurar desde la interfaz web o la CLI del CMM de Oracle ILOM.

Para obtener más información acerca de cómo configurar una política de redundancia de la fuente de alimentación para un chasis de sistema blade del CMM de Oracle ILOM, consulte el siguiente procedimiento.

▼ Configuración de política de redundancia de la fuente de alimentación del CMM

Antes de empezar

- Se requiere la versión de firmware 3.1.1 o posterior de CMM de Oracle ILOM.
- Se debe instalar inicialmente un mínimo de dos unidades de fuente de alimentación (PSU) en el chasis de sistema blade para admitir la política de redundancia de la fuente de alimentación.

Nota – Las PSU de Sun Blade 6000 contienen dos fases de energía. La PSU de Sun Blade 6048 contiene tres fases de energía. Los administradores del sistema pueden apagar una fase de la PSU mediante la activación de la política de gestión del sistema para Light Load Efficiency Mode (modo de eficiencia de carga de luz) (LLEM). El modo LLEM admite PSU redundantes y no redundantes.

- Se requiere el rol de Admin (a) en Oracle ILOM para modificar la propiedad de límite de otorgamiento de CMM.
- La política de redundancia de la fuente de alimentación controla la cantidad de energía que el CMM reserva de cada PSU en caso de que se produzca un fallo en la PSU. En Oracle ILOM, la política de fuente de alimentación del CMM está establecida de manera predeterminada a fin de reservar la mitad de la energía (N+N) de cada PSU. Si se produce un fallo en una PSU del chasis blade, el CMM asigna la energía reservada de la PSU restante para evitar una pérdida de energía a los componentes del sistema de chasis.

  Los administradores del sistema pueden elegir aceptar la política de redundancia de la fuente de alimentación predeterminada (N+N) o desactivarla.

Nota – Cuando se modifica la política de redundancia de PSU, la modificación afectará el vataje de energía que el CMM puede asignar a los servidores blade de CPU. Por ejemplo, cuando la política de redundancia está activada (N+N), el CMM reajustará la energía máxima permitida al vataje que las PSU pueden proporcionar menos el vataje que se reserva. Si la política de redundancia está desactivada y se produce un fallo en una PSU, el CMM reducirá el vataje para la energía máxima permitida del sistema. Si el vataje máximo permitido del sistema se reduce por debajo del vataje de energía ya asignado, el administrador del sistema debe realizar los pasos para apagar los servidores blade de CPU a fin de reducir la asignación de energía del chasis.

Este procedimiento proporciona instrucciones web y de la CLI del CMM.

● **Para definir la política de redundancia de la fuente de alimentación del CMM, realice uno de los siguientes procedimientos en la interfaz de Oracle ILOM:**

Interfaz de Oracle ILOM	Procedimiento para definir la política de redundancia de PSU del CMM
Web	a. Haga clic en Power Management (Gestión de energía) > Redundancy (Redundancia). b. Active una de las siguientes políticas de redundancia de energía: **N+N** (opción predeterminada): cuando está activada esta opción, el CMM reserva la mitad de la energía de cada PSU del chasis para redundancia de energía. O bien: **None** (Ninguno): cuando esta opción está activada, la configuración de la política de PSU de redundancia se desactiva. c. Haga clic en Save (Guardar) para aplicar los cambios.
CLI	■ Escriba: `set /CMM/powermgmt redundancy=`*redundancy*|*none* *Donde:* `redundancy` (predeterminado): cuando se establece, el CMM reserva la mitad de la energía de cada PSU del chasis para redundancia de energía. `none`: cuando se establece, la configuración de la política de PSU de redundancia se desactiva.

Más información

Información relacionada

- Forzar la velocidad del ventilador de la fuente de alimentación del CMM, “Políticas de gestión del sistema configurables desde el CMM” en la página 187
- Política de CMM para la gestión de energía del chasis, “Políticas de gestión del sistema configurables desde el CMM” en la página 187

Ejecución de tareas de gestión de configuración y mantenimiento de Oracle ILOM

Descripción	Vínculos
Consulte esta sección para obtener información acerca de cómo ejecutar actualizaciones de firmware para dispositivos actualizables del sistema.	■ "Ejecución de actualizaciones de firmware" en la página 201
Consulte esta sección para obtener información sobre cómo restablecer la energía en los componentes del SP, CMM o chasis blade.	■ "Restauración de la energía al procesador de servicio o al módulo de supervisión del chasis " en la página 210
Consulte esta sección para obtener instrucciones para realizar copias de seguridad, restaurar o restablecer la configuración del SP o CMM de Oracle ILOM.	■ "Copia de seguridad, restauración o restablecimiento de la configuración de Oracle ILOM" en la página 211

Información relacionada

- *User?s Guide*, Taking a Snapshot: Oracle ILOM SP State

Ejecución de actualizaciones de firmware

Para garantizar que los usuarios tengan acceso a las últimas funciones y mejoras del producto Oracle ILOM, todos los dispositivos actualizables del sistema deben actualizarse con la última versión de firmware de Oracle ILOM.

Los administradores del sistema pueden actualizar el firmware de todos los dispositivos actualizables del sistema que utilizan la interfaz web o la CLI de Oracle ILOM.

Para obtener más información acerca de las actualizaciones de firmware de Oracle ILOM, consulte estos temas:

- "Dispositivos actualizables de firmware" en la página 202
- "Conservación de la configuración de Oracle ILOM " en la página 202
- "Antes de comenzar la actualización de firmware" en la página 203
- "Actualización de la imagen de firmware del SP o CMM del servidor" en la página 204

- "Actualización de las imágenes de firmware de componentes de chasis blade" en la página 207
- "Recuperación de un error de red durante la actualización del firmware" en la página 210

Dispositivos actualizables de firmware

Las imágenes de firmware están disponibles en el sitio web de descarga de productos Oracle para los siguientes dispositivos gestionados de Oracle ILOM:

- Servidores blade o montados en bastidor (x86 y SPARC) que contienen un procesador de servicio (SP)
- Módulo de supervisión del chasis (CMM) del sistema blade
- Módulos de expansión de red (NEM) del chasis del sistema blade que incluyen un procesador de servicio
- Servidores blade de almacenamiento del chasis del sistema blade

Para obtener instrucciones para la descarga de firmware, consulte "Descarga de firmware y software de productos" en la página 8.

Conservación de la configuración de Oracle ILOM

Al realizar una actualización a una versión de firmware posterior, la opción Preserve Configuration (Conservar configuración) (cuando está activada) guarda la configuración existente de Oracle ILOM y restaura las opciones de configuración definidas por el usuario una vez finalizada la actualización de firmware. No obstante, cuando la opción Preserve Configuration no está activada, las opciones de configuración de Oracle ILOM (incluida la configuración de red) se restablecen a sus valores predeterminados de fábrica al finalizar el proceso de actualización de firmware.

Nota – El término *configuración* hace referencia a los ajustes que el usuario ha configurado en Oracle ILOM. Entre los ajustes se incluyen ajustes de cuentas de usuario, valores de red de SP, ajustes de acceso de gestión, ajuste de configuración de alertas y configuraciones de gestión remota, entre otros.

Si está actualizando a una versión anterior del firmware y Oracle ILOM detecta una configuración que se ha conservado para dicha versión, la opción Preserve Configuration (cuando esté activada) recuperará la configuración de la versión anterior una vez finalizado el proceso de actualización.

Por lo general, no debe actualizar el firmware del sistema a una versión anterior. Sin embargo, si considera que debe ejecutar una versión anterior del firmware en el sistema, puede actualizar el firmware a cualquier versión de firmware anterior que esté disponible para descargar.

Antes de comenzar la actualización de firmware

Antes de actualizar el firmware de Oracle ILOM, debe:

1. Verificar que el SP o CMM del servidor gestionado tenga conectividad para actualizar la imagen del firmware.

   Por ejemplo, para verificar que el SP o CMM del servidor esté conectado a la red, utilice un cliente de explorador web remoto o un cliente ssh de CLI remoto para iniciar sesión en el SP o CMM del servidor. Para obtener instrucciones, consulte "Inicio de sesión en el SP o CMM de Oracle ILOM" en la página 30.
2. Identificar la versión de firmware de Oracle ILOM que está en ejecución en el dispositivo gestionado (SP de servidor, servidor de almacenamiento, SP del NEM o CMM).

   La versión de firmware para todos los dispositivos actualizables se muestran en la página Firmware en la interfaz web o en el destino `/System/Firmware` de la CLI.
3. Descargar la imagen de firmware para el dispositivo actualizable desde el sitio web de descarga de productos Oracle y colocar la imagen en un recurso compartido local o de red o en un servidor TFTP, FTP, HTTP o HTTPS.

   Para obtener instrucciones para la descarga de firmware, consulte "Descarga de firmware y software de productos" en la página 8.
4. Obtener un nombre de usuario y una contraseña de Oracle ILOM con privilegios de cuenta del rol Admin (a). Debe tener privilegios de Admin (a) para actualizar la imagen de firmware.
5. Notificar a los usuarios de SP o CMM de la actualización programada de firmware y solicitarles que cierren todas las sesiones de cliente hasta que finalice la actualización de firmware.

   Los administradores del sistema pueden usar un mensaje de vista de título para comunicar este mensaje a los usuarios. Para obtener instrucciones para la creación y activación de un mensaje de vista de título al momento del inicio de sesión, consulte Tabla 42.
6. Si la plataforma del servidor host lo requiere, desactive el sistema operativo del host antes de actualizar la imagen de firmware del SP.

   Tenga en cuenta que si el servidor host está encendido y el servidor de plataforma requiere que esté apagado, debe hacer clic en el botón del panel Actions (Acciones) de la página web Summary (Resumen) para desactivar el servidor y el sistema operativo del host de manera habitual. De manera alternativa, puede realizar un cierre controlado del servidor y del sistema operativo del host desde la CLI mediante la ejecución del siguiente comando: **`stop /System`**

Actualización de la imagen de firmware del SP o CMM del servidor

Los administradores del sistema pueden elegir iniciar el proceso de actualización del firmware para dispositivos actualizables desde el panel Actions (Acciones) de la interfaz web, la página Maintenance (Mantenimiento) > Firmware Upgrade (Actualización de firmware) o un destino de CLI.

El siguiente procedimiento explica el proceso de actualización de firmware mediante la CLI y la página Maintenance de la interfaz web.

Antes de empezar

- Asegúrese de que se cumplan los requisitos iniciales para la actualización de la imagen de firmware del SP o CMM. Consulte "Antes de comenzar la actualización de firmware" en la página 203.
- El proceso de actualización del firmware dura varios minutos. Durante este tiempo, no realice otras tareas con Oracle ILOM. Cuando finalice el proceso de actualización de firmware, se reiniciará el sistema.

Para iniciar el proceso de actualización de firmware y verificar que el proceso de actualización haya finalizado correctamente, siga estos pasos:

1. **Para iniciar el proceso de actualización de firmware para una imagen del SP o CMM del servidor, realice los siguientes pasos mediante una de las interfaces de Oracle ILOM:**

Interfaz de Oracle ILOM	Para iniciar y ejecutar el procedimiento de actualización de firmware para el SP o CMM
Web	a. Haga clic en Maintenance (Mantenimiento) > Firmware Upgrade (Actualización de firmware). b. Haga clic en el botón Enter Firmware Upgrade Mode (Introducir modo de actualización de firmware), luego en OK (Aceptar) en el cuadro de diálogo de confirmación de actualización para continuar. La página Firmware Upgrade muestra la propiedad para cargar la imagen de firmware. **Nota**: si no se ha descargado la imagen de firmware del sitio web de descarga de productos Oracle, consulte estas instrucciones para descargar la imagen actualizada: "Descarga de firmware y software de productos" en la página 8. c. En la página Firmware Upgrade, lleve a cabo una de las siguientes acciones: Haga clic en Browse (Examinar) para especificar la imagen de firmware que se cargará y, a continuación, en el botón Upload (Cargar). O bien: Introduzca una URL para cargar la imagen de firmware y haga clic en el botón Upload. Oracle ILOM valida la imagen de firmware y luego muestra opciones en la página Firmware Verification (Comprobación de firmware). d. En la página Firmware Verification, active las opciones aplicables: **Preserve Configuration** (Conservar la configuración): active esta opción para guardar y restaurar la configuración existente del firmware de Oracle ILOM una vez finalizada la actualización de firmware. Para obtener más información sobre esta opción, consulte "Conservación de la configuración de Oracle ILOM " en la página 202. **Preserve BIOS Configuration (x86 server SPs only)** (Conservar configuración del BIOS [SP del servidor x86 solamente]): active esta opción para guardar y restaurar la configuración existente del BIOS una vez finalizado el proceso de actualización. Esta opción no se admite en todos los servidores x86. Por lo tanto, si no se presenta esta opción, Oracle ILOM restaura la configuración predeterminada del BIOS después de finalizar el proceso de actualización. **Delay BIOS Upgrade (x86 server SPs only)** (Posponer actualización del BIOS [SP del servidor x86 solamente]): active esta opción para posponer la actualización de BIOS de servidores x86 hasta la próxima vez que se apague y se vuelva a encender el sistema. e. Haga clic en Start (Iniciar) para iniciar el proceso de actualización. f. Haga clic en OK para continuar con una serie de indicaciones hasta que aparezca la página Update Status (Estado de la actualización). g. El sistema se reiniciará automáticamente cuando el estado de la actualización indique 100%. Para comprobar que la versión correcta de firmware esté en ejecución en el SP o CMM del servidor, consulte Paso 2 en el procedimiento.

Interfaz de Oracle ILOM	Para iniciar y ejecutar el procedimiento de actualización de firmware para el SP o CMM
CLI	a. Para cargar la imagen de firmware de Oracle ILOM mediante la CLI, ejecute el comando `load -source` seguido de la ruta para ubicar la imagen de firmware que desea instalar. Por ejemplo: **`load -source`** *protocol://username:password@server_ip/<path_to_image>/<image.pkg>* *Donde protocol* puede ser: *http*, *https*, *ftp*, *tftp*, *sftp*, *scp* Aparece una serie de indicaciones. b. Escriba **y** para cargar el archivo de imagen, luego escriba **y** para activar las opciones de actualización aplicables, por ejemplo: preserve SP configuration (Conservar configuración del SP), preserve x86 BIOS settings (Conservar configuración del BIOS de servidores x86), o delay the x86 BIOS update (Posponer actualización del BIOS de servidores x86) **Nota**: no todos los SP de servidores x 86 admiten la opción para conservar la configuración del BIOS. Si no se muestra la opción de BIOS de servidores x86, Oracle ILOM conservará automáticamente la configuración predeterminada del BIOS. Para obtener más información acerca de cómo conservar la configuración del SP, consulte “Conservación de la configuración de Oracle ILOM ” en la página 202. c. Oracle ILOM muestra un mensaje de estado cuando finaliza el proceso de firmware. El sistema se reiniciará automáticamente para aplicar la nueva imagen de firmware. Para comprobar que la versión correcta de firmware esté en ejecución en el SP del servidor, consulte Paso 2 en el procedimiento.

2 Para comprobar que la versión actualizada de firmware esté instalada, realice una de las siguientes acciones:

- **Web:**

  Inicie sesión en Oracle ILOM y haga clic en System Information (Información del sistema) > Firmware para ver la versión de firmware instalada.

  Nota – Una vez finalizada la actualización de firmware, es posible que la interfaz web de Oracle ILOM no se actualice correctamente. La falta de información en la página web de Oracle ILOM o la aparición de un mensaje de error pueden indicar que se visualiza una versión de la página de la memoria caché perteneciente a la versión anterior. Borre la memoria caché del explorador y actualícelo antes de continuar.

- **CLI:**

  Escriba: **`show /System/Firmware`**

Más información

Información relacionada:

- “Recuperación de un error de red durante la actualización del firmware” en la página 210
- Tabla 13

▼ Actualización de las imágenes de firmware de componentes de chasis blade

El CMM de Oracle ILOM ofrece una interfaz de usuario centralizada para gestionar las actualizaciones de firmware para los siguientes componentes de chasis blade actualizables.

- Servidores blade de almacenamiento
- Servidores blade de CPU
- NEM que contienen SP

Los administradores del sistema pueden elegir usar la interfaz web de CMM o la CLI para visualizar las versiones de firmware de componentes o iniciar actualizaciones de firmware de componentes de chasis.

El siguiente procedimiento explica el proceso para actualizar la imagen de firmware de un componente de chasis mediante la página Firmware Update (Actualización de firmware) de la interfaz web y los destinos de componentes de chasis de la CLI para cargar la actualización de firmware.

Antes de empezar

- Asegúrese de haber cumplido con los requisitos iniciales para la actualización de firmware. Consulte “Antes de comenzar la actualización de firmware” en la página 203.
- El proceso de actualización del firmware dura varios minutos. Durante este tiempo, no realice otras tareas con Oracle ILOM. Cuando finalice el proceso de actualización de firmware, se reiniciará el sistema.

Para iniciar el proceso de actualización de firmware y verificar que el proceso de actualización haya finalizado correctamente, siga estos pasos:

1 **Para iniciar el proceso de actualización de firmware para una imagen del SP o CMM del servidor, realice uno de los siguientes procedimientos de la interfaz de Oracle ILOM:**

Interfaz de Oracle ILOM	Para iniciar y ejecutar el procedimiento de actualización de firmware para componentes de chasis blade (blades o NEM)
Web	a. En la interfaz web del CMM, haga clic en Firmware. b. En la tabla, haga clic en el botón de radio ubicado junto al componente de chasis para el que desea actualizar el firmware; luego, haga clic en la opción Firmware Update (Actualización de firmware) en el cuadro de lista Actions (Acciones). La página Firmware Upgrade muestra la propiedad para cargar la imagen de firmware. c. En la página Firmware Upgrade, lleve a cabo una de las siguientes acciones: Haga clic en Browse (Examinar) para especificar la imagen de firmware que se cargará y, a continuación, en el botón Upload (Cargar). O bien: Introduzca una URL para cargar la imagen de firmware y haga clic en el botón Upload. Oracle ILOM valida la imagen de firmware y luego, según el componente de chasis, muestra un botón para iniciar el proceso de actualización de firmware o muestra opciones de configuración para los SP de servidores blade de CPU. Si actualiza el firmware para un SP de servidor blade de CPU, continúe con el paso 4; de lo contrario, continúe con el paso 5. d. (Actualización de blades de CPU solamente) En la página Firmware Verification (Comprobación de firmware), active las opciones aplicables disponibles para servidores blade de CPU: **Preserve Configuration** (Conservar la configuración): active esta opción para guardar y restaurar la configuración existente del firmware de Oracle ILOM una vez finalizada la actualización de firmware. Para obtener más información sobre esta opción, consulte "Conservación de la configuración de Oracle ILOM " en la página 202. **Preserve BIOS Configuration (x86 server SPs only)** (Conservar configuración del BIOS [SP del servidor x86 solamente]): active esta opción para guardar y restaurar la configuración existente del BIOS una vez finalizado el proceso de actualización. Esta opción no se admite en todos los servidores x86. Por lo tanto, si no se presenta esta opción, Oracle ILOM restaura la configuración predeterminada del BIOS después de finalizar el proceso de actualización. **Delay BIOS Upgrade (x86 server SPs only)** (Posponer actualización del BIOS [SP del servidor x86 solamente]): active esta opción para posponer la actualización de BIOS de servidores x86 hasta la próxima vez que se apague y se vuelva a encender el sistema. e. Haga clic en Start (Iniciar) para iniciar el proceso de actualización. f. Haga clic en OK para continuar con una serie de indicaciones hasta que aparezca la página Update Status (Estado de la actualización). g. El sistema se reiniciará automáticamente cuando el estado de la actualización alcance el 100%. Para comprobar que la versión correcta de firmware esté en ejecución en el SP o CMM del servidor, consulte Paso 2 en el procedimiento.

Interfaz de Oracle ILOM	Para iniciar y ejecutar el procedimiento de actualización de firmware para componentes de chasis blade (blades o NEM)
CLI	a. Navegue hasta el destino de firmware de blade o NEM, por ejemplo: **`cd /System/Firmware/Other_Firmware/Firmware_`***#* *Donde* **`Firmware_#`** es el número asignado al servidor blade o NEM específico. b. Para cargar la imagen de firmware de Oracle ILOM mediante la CLI, ejecute el comando `load` -source seguido de la ruta para ubicar la imagen de firmware que desea instalar. Por ejemplo: **`load -source`** *protocol://username:password@server_ip/<path_to_image>/<image.pkg>* *Donde protocol* puede ser: *http*, *https*, *ftp*, *tftp*, *sftp*, *scp*. Aparece un mensaje que le solicita que cargue la imagen. c. Escriba **`y`** para cargar el archivo de imagen. Continúe con el paso 4 para actualizaciones de firmware de blades de CPU; de lo contrario, continúe con el paso 5 para actualizaciones de firmware de NEM o blades de almacenamiento. d. (Actualización de blades de CPU solamente) Escriba **`y`** para activar las opciones de actualización aplicables, por ejemplo: preserve SP configuration (Conservar configuración del SP), preserve x86 BIOS settings (Conservar configuración del BIOS de servidores x86), o delay the x86 BIOS update (posponer actualización del BIOS de servidores x86) **Nota**: no todos los SP de servidores x 86 admiten la opción para conservar la configuración del BIOS. Si no se muestra la opción de BIOS de servidores x86, Oracle ILOM conservará automáticamente la configuración predeterminada del BIOS. Para obtener más información acerca de cómo conservar la configuración del SP, consulte “Conservación de la configuración de Oracle ILOM ” en la página 202. e. Oracle ILOM muestra un mensaje de estado cuando finaliza el proceso de firmware. El componente de chasis se reiniciará automáticamente para aplicar la nueva imagen de firmware. Para comprobar que esté instalada la versión correcta de firmware del componente de chasis, consulte Paso 2 en el procedimiento.

2 Para comprobar que la versión actualizada de firmware esté instalada, realice una de las siguientes acciones:

- **Web:**

  Inicie sesión en el CMM de Oracle ILOM y haga clic en System Information (Información del sistema) > Firmware para ver la versión de firmware instalada para cada componente de chasis actualizable.

  Nota – Una vez finalizada la actualización de firmware, es posible que la interfaz web de Oracle ILOM no se actualice correctamente. La falta de información en la página web de Oracle ILOM o la aparición de un mensaje de error pueden indicar que se visualiza una versión de la página de la memoria caché perteneciente a la versión anterior. Borre la memoria caché del explorador y actualícelo antes de continuar.

- **CLI:**

  Escriba: **show /System/Firmware/Other_Firmware/Firmware_***n*

Más información Información relacionada:

- "Recuperación de un error de red durante la actualización del firmware" en la página 210
- Tabla 13

▼ Recuperación de un error de red durante la actualización del firmware

Si se produce un error en la red al realizar una actualización de firmware, Oracle ILOM automáticamente agota el tiempo de espera de la sesión y reinicia el sistema. Una vez reiniciado el sistema, siga estas directrices para recuperar el proceso de actualización de firmware.

1. **Examine y solucione el problema de red.**

2. **Vuelva a conectar el SP o CMM de Oracle ILOM.**

3. **Reinicie el proceso de actualización del firmware.**

Restauración de la energía al procesador de servicio o al módulo de supervisión del chasis

En algunas ocasiones, se debe restablecer el módulo de supervisión del chasis (CMM) del blade o el procesador de servicio (SP) para un servidor o un módulo de ampliación de red (NEM) para completar una actualización o para borrar un estado de error. La operación de restablecimiento del SP y CMM se parece al restablecimiento de un equipo en el que todos los procesos activos se interrumpen y se reinicia el sistema.

Al reiniciar un SP o CMM del servidor, se desconectan automáticamente todas las sesiones actuales de Oracle ILOM y el procesador de servicio no puede gestionarse hasta que el proceso de restablecimiento se complete. Sin embargo, el sistema operativo del host en un servidor no se ve afectado cuando se reinicia un SP de servidor blade de CPU o un SP de servidor montado en bastidor.

Los administradores del sistema puede reiniciar el CMM, el SP de NEM y el SP del servidor desde la interfaz web o la CLI. Para obtener más instrucciones para reiniciar el CMM y el SO, consulte el siguiente procedimiento.

▼ Restablecimiento de la energía al CMM, SP de NEM o SP del servidor

Antes de empezar

- Ser requiere el rol Host Control and Reset (Restablecimiento y control del host) (r) para reiniciar un SP o CMM.
- Después de hacer clic en el botón web Reset (Restablecer) o ejecutar el comando `reset` de la CLI, Oracle ILOM automáticamente mostrará una solicitud para confirmar la operación de restablecimiento, a menos que se especifique una opción `-script` de la CLI (**`reset`** *[options] target*).

Este procedimiento proporciona instrucciones web y de la CLI.

● **Para restablecer la energía a un SP o CMM, realice una de las siguientes acciones:**

Interfaz de Oracle ILOM	Restablecimiento de la energía al SP o CMM
Web	Elija una de estas posibilidades: ■ **SP del servidor**: Haga clic en ILOM Administration (Administración de ILOM) > Maintenance (Mantenimiento) > Reset SP (Restablecer SP) y luego en el botón Reset SP. ■ **Componentes de chasis blade y CMM**: Haga clic en ILOM Administration > Maintenance >Reset Components (Restablecer componentes). Haga clic en el botón de radio ubicado junto al componente del chasis (CMM, blade, NEM) y luego en el botón Reset.
CLI	Elija una de estas posibilidades: ■ **SP del servidor**: Para restablecer el SP del servidor, escriba: **`reset /SP`** ■ **Componentes de chasis blade y CMM**: Para restablecer el CMM, escriba: **`reset /CMM`** Para restablecer un SP blade, escriba: **`reset /Servers/Blades/BL`*n*`/SP`** Para restablecer un SP de NEM, escriba: **`reset /System/IO_Modules/NEM`*n*`/SP`**

Copia de seguridad, restauración o restablecimiento de la configuración de Oracle ILOM

Las propiedades de copia de seguridad y restablecimiento proporcionadas en Oracle ILOM permiten a los administradores del sistema copiar la configuración actual de Oracle ILOM en un archivo XML de copia de seguridad y restaurar la configuración cuando sea necesario. Los administradores del sistema pueden optar por usar el archivo de configuración XML de copia de seguridad para restaurar la configuración en el SP o CMM presente o por utilizarlo para instalar las opciones de configuración en otros CMM o SP del servidor.

Las propiedades predeterminadas de restablecimiento proporcionadas en Oracle ILOM permiten a los administradores del sistema borrar cualquiera de las propiedades de configuración de Oracle ILOM definidas por el usuario y restaurarlas a los valores predeterminados de fábrica.

Los administradores del sistema pueden realizar una copia de seguridad y restaurar la configuración de Oracle ILOM, y restablecer las opciones de configuración a los valores predeterminados desde la interfaz web o la CLI. Para obtener más información acerca del uso de las funciones predeterminadas de copia de seguridad, restauración y restablecimiento de Oracle ILOM, consulte los siguientes temas:

- "Uso de operaciones predeterminadas de copia de seguridad, restauración y restablecimiento" en la página 212
- "El rol de usuario determina los valores de configuración de copia de seguridad y restauración. " en la página 213
- "Copia de seguridad de la configuración de Oracle ILOM" en la página 213
- "Edición opcional del archivo de configuración XML de copia de seguridad de Oracle ILOM " en la página 215
- "Restauración del archivo XML de copia de seguridad de Oracle ILOM" en la página 217
- "Restablecimiento de la configuración de Oracle ILOM a la configuración predeterminada de fábrica" en la página 219

Uso de operaciones predeterminadas de copia de seguridad, restauración y restablecimiento

Los administradores del sistema pueden usar las operaciones predeterminadas de copia de seguridad, restauración y restablecimiento en las siguientes formas:

Replicación de la configuración de Oracle ILOM para utilizarla en otros sistemas.
Los administradores del sistema pueden replicar la configuración de Oracle ILOM para utilizarla en otros CMM o SP de servidor Oracle realizando estos pasos: 1. Personalice la configuración de Oracle ILOM según sea necesario Por ejemplo, defina cuentas de usuario, modifique opciones de configuración predeterminadas de red, establezca notificaciones de alerta, defina políticas del sistema, etc. 2. Guarde la configuración de Oracle ILOM en un archivo XML de copia de seguridad. 3. Edite el archivo XML de copia de seguridad para eliminar los ajustes que son únicos para un sistema en particular (por ejemplo, la dirección IP). 4. Realice una operación de restauración para replicar la configuración en otros CMM o SP de servidor Oracle.
Recupere una configuración activa de Oracle ILOM cuando la configuración existente de Oracle ILOM ya no funciona.

Si se realizaron modificaciones a la configuración de Oracle ILOM desde la última operación de copia de seguridad y la configuración actual de Oracle ILOM ya no funciona, los administradores del sistema pueden recuperar la configuración de copia de seguridad funcional mediante estos pasos:

1. Restablezca los valores predeterminados de la configuración de Oracle ILOM.
2. Restaure la configuración de Oracle ILOM a la última configuración funcional.

El rol de usuario determina los valores de configuración de copia de seguridad y restauración.

Por razones de seguridad, los privilegios del rol de usuario asignados actualmente a la cuenta de usuario utilizada para realizar copia de seguridad o restaurar el archivo de configuración XML determinan los valores de configuración que se incluyen en la operación de copia de seguridad o restauración.

Para asegurarse de que se restauren todos los valores de configuración de un archivo XML o se realice una copia de seguridad de todos ellos, se requieren privilegios completos del rol de usuario. Por lo tanto, los administradores del sistema que realizan operaciones de copia de seguridad y restauración deben tener un rol de perfil de administrador (`administrator`) asignado o todos los siguientes roles de usuario asignados:

- Admin (Administrador) (`a`)
- User Management (Gestión de usuarios) (`u`)
- Console (c) (Consola)
- Reset and Host Control (Restablecimiento y control del host) (`r`)
- Read Only (Sólo lectura) (`o`)

Si se utiliza una cuenta de usuario con privilegios insuficientes para realizar una operación de copia de seguridad o restauración, es posible que algunas opciones de configuración no se restauren o no se realice copia de seguridad de ellas. Para cada propiedad de configuración que no se restaure o de la que no se haya realizado copia de seguridad debido a la falta de privilegios de usuario, se crea una entrada de registro en el registro de eventos de Oracle ILOM.

Para obtener una lista de descripciones de roles de usuario en Oracle ILOM, consulte Tabla 9. Para obtener instrucciones para asignar roles de usuario, consulte “Configuración de cuentas de usuario locales ” en la página 46.

Para obtener información detallada sobre cómo visualizar y filtrar los eventos que registra Oracle ILOM, consulte la *User?s Guide*, Managing Oracle ILOM Log Entries.

▼ Copia de seguridad de la configuración de Oracle ILOM

Los administradores del sistema pueden guardar una copia de seguridad del archivo de configuración de Oracle ILOM que se ejecuta activamente en el CMM o SP del servidor. Al iniciar una operación de copia de seguridad, todas las sesiones de clientes de Oracle ILOM en el

SP o CMM se suspenden temporalmente. Las sesiones suspendidas se reanudan en operación normal una vez que se haya completado la operación de copia de seguridad. Una operación de copia de seguridad normalmente tarda entre dos y tres minutos en completarse.

Antes de empezar

- Para realizar una operación de copia de seguridad de configuración en Oracle ILOM, se requiere el rol de perfil de Administrador (`administrator`) o se deben asignar los siguientes roles de usuario: Admin (`a`), User Management (Gestión de usuarios) (`u`), Console (Consola) (`c`) Reset and Host Control (Restablecimiento y control del host) (`r`) y Read Only (Sólo lectura) (`o`).

  Para obtener más información, consulte "El rol de usuario determina los valores de configuración de copia de seguridad y restauración. " en la página 213.

El siguiente procedimiento de copia de seguridad de configuración de Oracle ILOM ofrece instrucciones web y de la CLI para el SP y el CMM.

● Para realizar una copia de seguridad de la configuración de Oracle ILOM a un archivo XML, realice los siguientes pasos para una de las interfaces de usuario de Oracle ILOM enumeradas.

Interfaz de usuario de Oracle ILOM	Copia de seguridad de la configuración de Oracle ILOM a un archivo XML
Web	a. Haga clic en ILOM Administration (Administración de ILOM)> Configuration Management (Gestión de la configuración) > Backup/Restore (Copia de seguridad/restauración). b. Haga clic en Backup, en el cuadro Operations (Operaciones). c. Haga clic en el cuadro Transfer Method (Método de transferencia) para especificar un método para transferir el archivo de configuración de Oracle ILOM. Para obtener descripciones de propiedades para cada método de transferencia de archivo, consulte Tabla 13. d. Para cifrar el archivo de configuración de copia de seguridad, escriba una contraseña en el cuadro de texto Passphrase (Contraseña) y luego vuelva a escribir la contraseña en el cuadro de texto Confirm Passphrase (Confirmar contraseña). El archivo de copia de seguridad se cifra usando la contraseña especificada. **Nota**: para realizar una copia de seguridad de datos confidenciales como contraseñas, claves de SSH, certificados y LDoms, debe especificar una contraseña. e. Haga clic en Run (Ejecutar) para iniciar la operación de copia de seguridad. Al ejecutar la operación de copia de seguridad, las sesiones de clientes de Oracle ILOM en el SP o CMM se suspenden temporalmente. Las sesiones se reanudarán en operación normal una vez se haya completado la operación de copia de seguridad.

Interfaz de usuario de Oracle ILOM	Copia de seguridad de la configuración de Oracle ILOM a un archivo XML
CLI	a. Navegue hasta el destino `config` de la CLI, por ejemplo: **`cd /SP/config`** **`cd /CMM/config`** b. Para cifrar el archivo de configuración de copia de seguridad, establezca el valor a para la propiedad de la contraseña, por ejemplo: **`set passphrase=`***value* El archivo de copia de seguridad se cifra usando la contraseña especificada. **Nota**: para realizar una copia de seguridad de datos confidenciales como contraseñas, claves de SSH, certificados y LDoms, debe especificar una contraseña. c. Para iniciar la operación de copia de seguridad, escriba el siguiente comando desde dentro del directorio `/SP/config` o `/CMM/config`. Por ejemplo: **`set`** **`dump_uri=`***transfer_method***`://u`***sername:password@ipaddress_or_hostname***`/`***directorypath***`/`***filename* Donde *transfer method* puede ser: tftp, ftp, sftp, scp, http o https Para obtener descripciones de propiedades para cada método de transferencia de archivo, consulte Tabla 13. **Por ejemplo:** **`set dump_uri=scp://adminuser:userpswd@1.2.3.4/Backup/Lab9/SP123.config`** Al ejecutar la operación de copia de seguridad, las sesiones de clientes de Oracle ILOM en el SP o CMM se suspenden temporalmente. Las sesiones se reanudarán en operación normal una vez se haya completado la operación de copia de seguridad.

Más información

Información relacionada:

- "Edición opcional del archivo de configuración XML de copia de seguridad de Oracle ILOM " en la página 215
- "Restauración del archivo XML de copia de seguridad de Oracle ILOM" en la página 217
- "Uso de operaciones predeterminadas de copia de seguridad, restauración y restablecimiento" en la página 212

▼ Edición opcional del archivo de configuración XML de copia de seguridad de Oracle ILOM

Los usuarios avanzados pueden utilizar el archivo XML de copia de seguridad para aprovisionar otros CMM o SP del servidor Oracle en la red con la misma configuración de Oracle ILOM. Antes de utilizar un archivo XML de copia de seguridad en otro sistema, los administradores del sistema deben editar el archivo para eliminar cualquier información única a un sistema particular (por ejemplo, la dirección IP).

Archivo XML de ejemplo:

A continuación se ofrece un ejemplo de un archivo XML de copia de seguridad. El contenido del archivo se ha abreviado para este procedimiento.

```
<SP_config version="3.0">
<entry><entry><property>/SP/clock/datetime</property><value>Mon May 12 15:31:09 2010</value></entry>...
<property>/SP/check_physical_presence</property><entry><property>/SP/config/passphrase</property><value encrypted="tru
<value>false</value><entry><property>/SP/network/pendingipaddress</property><value>1.2.3.4</value></entry>...
</entry><entry><property>/SP/network/commitpending</property><value>true</value></entry>...
<entry><entry><property>/SP/services/snmp/sets</property><value>enabled</value></entry>...
<property>/SP/hostname</property><entry><property>/SP/users/john/role</property><value>aucro</value></entry><entry><pr
<value>labysystem12</value>
</entry>
<entry>
<property>/SP/system_identifier</property>
<value>SUN BLADE X8400 SERVER MODULE, ILOM v3.0.0.0, r32722</value>
</entry>
.
.
.
```

1 **Tenga en cuenta lo siguiente al examinar el archivo XML de ejemplo:**

- Los valores de configuración, excepto las contraseñas y las frases de contraseña, se encuentran en texto no cifrado.
- La propiedad `check_physical_presence`, que es la primera entrada de configuración del archivo, se establece en `false`. El valor predeterminado es `true`, de modo que este valor representa un cambio en la configuración predeterminada de Oracle ILOM.
- Los valores de configuración para `pendingipaddress` y `commitpending` son únicos de cada servidor. Estos valores deben eliminarse antes de usar el archivo XML de copia de seguridad para una operación de restauración en otro servidor.
- La cuenta de usuario `john` se configura con las funciones `a`, `u`, `c`, `r`, `o`. La configuración predeterminada de Oracle ILOM *no* tiene ninguna cuenta de usuario configurada, de modo que esta cuenta representa un cambio en la configuración predeterminada de Oracle ILOM.
- La propiedad `sets` de SNMP está establecida en Enabled (Activada). El valor predeterminado es que esté desactivada.

2 **Para modificar los valores de configuración que están en texto no cifrado, cámbielos o añada otros nuevos.**

Por ejemplo:

- **Para cambiar los roles asignados al usuario `john`, cambie el texto de la siguiente manera:**

```
<entry>
<property>/SP/users/john/role</property>
```

```
<value>auo</value>
</entry>
```

- **Para agregar una nueva cuenta de usuario y asignarla a los roles `a`, `u`, `c`, `r`, `o`, agregue el texto siguiente directamente debajo de la entrada del usuario `john`:**

  ```
  <entry>
  <property>/SP/users/bill/role</property>
  <value>aucro</value>
  </entry>
  ```

- **Para cambiar una contraseña, elimine el valor `encrypted="true"` y la cadena de contraseña cifrada y escriba la nueva contraseña. Por ejemplo, para cambiar la contraseña para el usuario `john`, cambie el archivo XML de la siguiente manera:**

  Cambie:

  ```
  <entry>
  <property>/SP/users/john/password</property>
  <value encrypted="true">c21f5a3df51db69fdf</value>
  </entry>
  ```

  Por:

  ```
  <entry>
  <property>/SP/users/john/password</property>
  <value>newpassword</value>
  </entry>
  ```

3 **Después de realizar los cambios en el archivo XML de copia de seguridad, guarde el archivo para que se puede utilizar en la operación de restauración en el mismo sistema o en un sistema diferente.**

Más información

Temas relacionados

- "Edición opcional del archivo de configuración XML de copia de seguridad de Oracle ILOM " en la página 215
- "Restauración del archivo XML de copia de seguridad de Oracle ILOM" en la página 217
- "Uso de operaciones predeterminadas de copia de seguridad, restauración y restablecimiento" en la página 212

▼ Restauración del archivo XML de copia de seguridad de Oracle ILOM

Los administradores del sistema pueden ejecutar una operación de restauración para recuperar el archivo XML desde un sistema remoto, analizar el contenido y actualizar el SP (o CMM) con los datos de configuración de la copia de seguridad. Al iniciar una operación de restauración, todas las sesiones de clientes de Oracle ILOM en el SP o CMM del servidor se suspenden

temporalmente. Las sesiones suspendidas se reanudan en operación normal una vez se haya completado la operación de restauración. Una operación de Restaurar normalmente tarda dos o tres minutos en completarse.

Antes de empezar

- Para realizar una operación de restauración de configuración en Oracle ILOM, se requiere el rol de perfil de administrador (`administrator`) o se deben asignar los siguientes roles de usuario: Admin (`a`), User Management (Gestión de usuarios) (`u`), Console (Consola) (`c`) Reset and Host Control (Restablecimiento y control del host) (`r`) y Read Only (Sólo lectura) (`o`).

  Para obtener más información, consulte "El rol de usuario determina los valores de configuración de copia de seguridad y restauración. " en la página 213.

El siguiente procedimiento de restauración de configuración de Oracle ILOM ofrece instrucciones web y de la CLI para el SP y el CMM.

● **Para restaurar el archivo XML de configuración de Oracle ILOM de copia de seguridad, realice los siguientes pasos para una de las interfaces de usuario de Oracle ILOM enumeradas.**

Interfaz de usuario de Oracle ILOM	Restauración de una copia de seguridad de la configuración de Oracle ILOM
Web	a. Haga clic en ILOM Administration (Administración de ILOM)> Configuration Management (Gestión de la configuración) > Backup/Restore (Copia de seguridad/restauración). b. Haga clic en Restore (Restauración) en el cuadro Operations (Operaciones). c. Haga clic en el cuadro Transfer Method (Método de transferencia) para especificar un método para transferir el archivo de configuración de Oracle ILOM. Para obtener descripciones de propiedades para cada método de transferencia de archivo, consulte Tabla 13. d. Si el archivo de configuración de copia de seguridad se cifró con una contraseña, escriba la contraseña en el cuadro de texto Passphrase (Contraseña) y luego, vuelva a escribir la contraseña en el cuadro de texto Confirm Passphrase (Confirmar contraseña). **Nota**: la contraseña introducida debe coincidir con la contraseña utilizada para cifrar el archivo de configuración de copia de seguridad. e. Haga clic en Run (Ejecutar) para iniciar la operación de restauración. Al ejecutar la operación de restauración, las sesiones de clientes de Oracle ILOM en el SP o CMM se suspenden temporalmente. Las sesiones se reanudarán en operación normal una vez se haya completado la operación de restauración.

Interfaz de usuario de Oracle ILOM	Restauración de una copia de seguridad de la configuración de Oracle ILOM
CLI	a. Navegue hasta el destino `config` de la CLI, por ejemplo: **`cd /SP/config`** **`cd /CMM/config`** b. Si el archivo de configuración de copia de seguridad se cifró con una contraseña, establezca el valor de la propiedad de contraseña a la contraseña utilizada para cifrar el archivo, por ejemplo: **`set passphrase=`***value* **Nota**: la contraseña introducida debe coincidir con la contraseña utilizada para cifrar el archivo de configuración de copia de seguridad. c. Para iniciar la operación de restauración, escriba el siguiente comando desde dentro del directorio `/SP/config` o `/CMM/config`. Por ejemplo: **`set`** **`load_uri=`***transfer_method*`://`*username:password@ipaddress_or_hostname/directorypath/filename* Donde *transfer method* puede ser: tftp, ftp, sftp, scp, http o https. Para obtener descripciones de propiedades para cada método de transferencia de archivo, consulte Tabla 13. **Por ejemplo:** set load_uri=scp://adminuser:userpswd@1.2.3.4/Backup/Lab9/SP123.config Al ejecutar la operación de restauración, las sesiones de clientes de Oracle ILOM en el SP o CMM se suspenden temporalmente. Las sesiones se reanudarán en operación normal una vez se haya completado la operación de restauración.

Más información

Información relacionada:

- "Uso de operaciones predeterminadas de copia de seguridad, restauración y restablecimiento" en la página 212
- "Restauración del archivo XML de copia de seguridad de Oracle ILOM" en la página 217
- "El rol de usuario determina los valores de configuración de copia de seguridad y restauración. " en la página 213

▼ Restablecimiento de la configuración de Oracle ILOM a la configuración predeterminada de fábrica

Los administradores del sistema pueden restaurar los valores de configuración actuales de Oracle ILOM en el SP o el CMM a los valores predeterminados originales de fábrica.

Para obtener una descripción de los valores posibles que puede establecer para una operación Reset to Defaults (Restablecer valores predeterminados), consulte la siguiente tabla.

Reset Property Value	Descripción
All (Todos)	Establezca la opción All para restablecer todos los datos de configuración de Oracle ILOM a los valores predeterminados en el próximo reinicio del procesador de servicio. Esta acción no borra las entradas del archivo de registro.
Factory (Fábrica)	Establezca la opción Factory para restablecer todos los datos de configuración de Oracle ILOM a los valores predeterminados y borrar los todos los archivos de registro en el próximo reinicio del procesador de servicio.
None (Ninguno) (valor predeterminado)	Establezca la opción None para la operación normal al usar las configuraciones actuales. O utilice la opción None para cancelar una operación Reset to Defaults pendiente (All o Factory) antes del próximo reinicio del procesador de servicio.

- **Para realizar una operación Reset to Defaults en un CMM o SP del servidor, realice los pasos siguientes para una de las interfaces de usuario de Oracle ILOM enumeradas.**

Interfaz de Oracle ILOM	Operación de restablecimiento a valores predeterminados para SP o CMM
Web	a. Haga clic en ILOM Administration (Administración de ILOM)> Configuration Management (Gestión de la configuración) > Reset Defaults (Restablecer valores predeterminados) b. Haga clic en el cuadro de lista Reset Defaults (Restablecer valores predeterminados) para especificar uno de los siguientes valores: *None*, *All* o *Factory*. c. Haga clic en el botón Reset Defaults.
CLI	Elija una de estas posibilidades: ■ **SP del servidor**: Escriba: **`set /SP reset_to_defaults=`***all*|*none*|*factory* ■ **CMM**: Escriba: **`set /CMM reset_to_defaults=`***all*|*none*|*factory*

Más información

Información relacionada:

- “Restauración de la energía al procesador de servicio o al módulo de supervisión del chasis ” en la página 210

Mantenimiento de parámetros de configuración del BIOS en un servidor x86

Descripción	Vínculos
Consulte este tema para identificar las maneras en que puede gestionar la configuración del BIOS en un servidor x86.	■ "Gestión de configuración del BIOS" en la página 221
Consulte estos temas para obtener información sobre las características, la terminología y las propiedades de configuración del BIOS en Oracle ILOM.	■ "Oracle ILOM: características de configuración del BIOS" en la página 222 ■ "Oracle ILOM: terminología del BIOS" en la página 223 ■ "Web y CLI: propiedades del BIOS" en la página 223
Consulte esta sección para obtener información sobre cómo realizar las tareas de configuración del BIOS desde Oracle ILOM.	■ "Realización de tareas de configuración del BIOS desde Oracle ILOM" en la página 229

Información relacionada

- Guía de administración para el servidor x86 de Sun, Oracle System Assistant
- Guía de administración para el servidor x86 de Sun, utilidad de configuración del BIOS

Gestión de configuración del BIOS

Los parámetros de configuración del BIOS se pueden gestionar en un servidor x86 de Oracle desde la utilidad de configuración del BIOS del host, la interfaz de Oracle System Assistant, y la CLI y la interfaz web de Oracle ILOM. Los siguientes temas de esta sección describen cómo gestionar la configuración del BIOS desde las interfaces de Oracle ILOM.

- "Oracle ILOM: características de configuración del BIOS" en la página 222
- "Oracle ILOM: consideraciones especiales del BIOS " en la página 222
- "Oracle ILOM: terminología del BIOS" en la página 223
- "Web y CLI: propiedades del BIOS" en la página 223

Nota – Para obtener instrucciones sobre cómo gestionar la configuración del BIOS desde la utilidad de configuración del BIOS del host o desde Oracle System Assistant, consulte la guía de administración del servidor x86 de Oracle.

Oracle ILOM: características de configuración del BIOS

Oracle ILOM proporciona un conjunto de propiedades configurables que ayudan a gestionar los parámetros de configuración del BIOS en un servidor x86 gestionado de Oracle ILOM. Estas propiedades configurables de Oracle ILOM permiten realizar las siguientes tareas:

- Realizar una copia de seguridad de los parámetros de configuración en el almacén de datos no volátiles del BIOS.
- Restaurar una copia de seguridad de los parámetros de configuración en el almacén de datos no volátiles del BIOS.
- Restablecer los parámetros del almacén de datos no volátiles del BIOS a los valores predeterminados de fábrica.

Además, Oracle ILOM supervisa de manera dinámica los parámetros del almacén de datos no volátiles del BIOS para garantizar que estén sincronizados con los parámetros del archivo de configuración del BIOS de Oracle ILOM. El estado de sincronización de la configuración, que aparece en la CLI y en la interfaz web, indica el estado actual de los parámetros del BIOS almacenados en el archivo de configuración del BIOS de Oracle ILOM.

Nota – En el caso de los usuarios avanzados que necesitan aprovisionar la configuración del BIOS en otro servidor x86 de Oracle, consulte “Edición opcional del archivo de configuración XML de copia de seguridad de Oracle ILOM ” en la página 215.

Oracle ILOM: consideraciones especiales del BIOS

- La configuración del BIOS de Oracle ILOM puede aumentar los tiempos de inicio del host cuando el archivo de configuración del BIOS de Oracle ILOM no está sincronizado con el almacén de datos no volátiles del BIOS del host.
- La actualización del firmware de Oracle ILOM en el SP del servidor puede afectar los parámetros de configuración del BIOS de Oracle ILOM cuando está activada la opción “Preserve existing BIOS configuration” (Conservar configuración existente del BIOS). Para obtener más detalles sobre cómo realizar una actualización del firmware y cómo conservar los parámetros de configuración del BIOS mantenidos por Oracle ILOM, consulte “Ejecución de actualizaciones de firmware” en la página 201.

Oracle ILOM: terminología del BIOS

Término de Oracle ILOM	Descripción
BIOS	El BIOS de un servidor x86 de Oracle es el programa de firmware de inicio que controla el sistema desde el momento en que el servidor host se enciende hasta que el sistema operativo toma el control. El BIOS almacena la fecha, la hora y la información de configuración del sistema en un almacén de datos no volátiles con alimentación por batería.
Versión del BIOS	Propiedad de sólo lectura que indica la versión de firmware actual del BIOS instalada en un servidor x86 de Oracle.
Almacén de datos no volátiles del BIOS	Los parámetros de configuración del BIOS del servidor x86 de Oracle que están almacenados actualmente en el chip de memoria no volátil.
Archivo de configuración del BIOS de Oracle ILOM	Archivo XML con mantenimiento dinámico en el SP del servidor que contiene una lista de los parámetros de configuración del BIOS que se recuperaron por última vez del almacén de datos no volátiles del BIOS.
Copia de seguridad de configuración del BIOS	Las propiedades configurables en Oracle ILOM que permiten recuperar una copia de los parámetros definidos actualmente en el almacén de datos no volátiles del BIOS y guardarlos en el archivo de configuración del BIOS de Oracle ILOM, en el SP del servidor.
Restauración de configuración del BIOS	Las propiedades configurables en Oracle ILOM que permiten exportar los parámetros del archivo de configuración del BIOS de Oracle ILOM al almacén de datos no volátiles del BIOS.
Parámetros de configuración del BIOS	Por lo general, los parámetros de configuración del BIOS copiados o exportados por Oracle ILOM incluyen los valores de configuración, lista de inicio y dispositivos de inicio.

Web y CLI: propiedades del BIOS

- Tabla 71
- Tabla 72
- Tabla 73

TABLA 71 Navegación web y destinos de CLI del BIOS

Navegación web	Destinos de CLI
System Management (Gestión del sistema) > BIOS	`/System/BIOS` `/System/BIOS/Config`

TABLA 72 Propiedades de web y CLI del BIOS

Nombre de la propiedad	Tipo	Valores	Descripción
System BIOS Version (Versión del BIOS del sistema) `(system_bios_version=)`	Sólo lectura		La propiedad System BIOS Version identifica la versión de firmware del BIOS que está instalada actualmente en el servidor x86 gestionado de Oracle.
BIOS Configuration: Sync Status (Configuración del BIOS: Estado de sincronización) `(config_sync_status=)`	Sólo lectura	*OK*|*Reboot Required*|*Internal Error*	La propiedad BIOS Configuration: Sync Status indica uno de los siguientes estados: ■ **OK** (Correcto). Los parámetros de configuración del BIOS mantenidos por Oracle ILOM están sincronizados con los parámetros de configuración del almacén de datos no volátiles del BIOS. ■ **Reboot Required** (Reinicio necesario). Los parámetros de configuración del BIOS mantenidos por Oracle ILOM no están sincronizados con los parámetros de configuración del almacén de datos no volátiles del BIOS. Se debe reiniciar el servidor x86 de Oracle para sincronizar los parámetros del BIOS. ■ **Internal Error** (Error interno). Oracle ILOM no puede leer el almacén de datos no volátiles del BIOS y esto le impide iniciar una operación de copia de seguridad o restauración del BIOS. Para obtener más ayuda, póngase en contacto con el servicio de asistencia de Oracle.
BIOS Configuration: Reset To Defaults (Configuración del BIOS: Restablecer valores predeterminados) `(reset_to_defaults=)`	Lectura|Escritura	*Factory* |*None*	La propiedad Reset To Defaults proporciona uno de los siguientes valores: ■ **Factory** (Fábrica). Establece los parámetros de configuración del almacén de datos no volátiles del BIOS en los valores predeterminados de fábrica. ■ **None** (Ninguno). Este valor aparece tras restablecer los parámetros del almacén de datos no volátiles del BIOS a los valores predeterminados de fábrica.

TABLA 72 Propiedades de web y CLI del BIOS *(Continuación)*

Nombre de la propiedad	Tipo	Valores	Descripción
BIOS Configuration: Backup (Configuración del BIOS: Copia de seguridad) (**dump_uri=**)	Sólo escritura		La propiedad BIOS Configuration: Backup permite crear una copia de los parámetros del almacén de datos no volátiles del BIOS y guardar esos parámetros en un archivo de configuración del BIOS, en el sistema de archivos de Oracle ILOM. Para obtener instrucciones sobre cómo realizar una copia de seguridad de la configuración del BIOS, consulte "Copia de seguridad de la configuración del BIOS " en la página 234.

TABLA 72 Propiedades de web y CLI del BIOS *(Continuación)*

Nombre de la propiedad	Tipo	Valores	Descripción
BIOS Configuration: Restore Status (Configuración del BIOS: Estado de restauración) (restore_status=)	Sólo lectura	OK | Restore pending | Partial restore: invalid configuration entry | Partial restore: invalid boot order entry | Partial restore: invalid configuration and boot order entries	La propiedad BIOS Configuration: Restore Status indica uno de los siguientes estados: ■ **OK** (Correcto). La última operación de restauración restableció correctamente los parámetros de configuración del BIOS de Oracle ILOM en el almacén de datos no volátiles del BIOS del host. ■ **Restore pending** (Restauración pendiente). El apagado del host está pendiente en la operación de restauración. **Nota**. Oracle ILOM lleva a cabo la operación de restauración cuando el servidor host está apagado. ■ **Partial restore: invalid configuration entry** (Restauración parcial: entrada de configuración no válida). La última operación de restauración no pudo restablecer uno o varios de los parámetros de configuración del BIOS del host. ■ **Partial restore: invalid boot order entry** (Restauración parcial: entrada de orden de inicio no válida). La última operación de restauración no pudo restablecer uno o varios dispositivos de inicio de la lista de orden de inicio del host. ■ **Partial restore: invalid configuration and boot order entries** (Restauración parcial: entradas de configuración y de orden de inicio no válidas). La última operación de restauración no pudo restablecer uno o varios parámetros de configuración del BIOS y uno o varios dispositivos de inicio de la lista de orden de inicio del host.

TABLA 72 Propiedades de web y CLI del BIOS *(Continuación)*

Nombre de la propiedad	Tipo	Valores	Descripción
BIOS Configuration: Restore (Configuración del BIOS: Restaurar) (`load_uri=` *restore_options*)	Lectura|Escritura	All| Configuration only| Bootlist only | Cancel Restore	La propiedad BIOS Configuration: Restore permite restaurar los parámetros del BIOS guardados anteriormente por Oracle ILOM en el almacén de datos no volátiles del BIOS del host. Las opciones para restaurar los parámetros del BIOS incluyen: ■ **All** (Todos). Restaura todos los parámetros de configuración del BIOS guardados anteriormente por Oracle ILOM. ■ **Configuration only** (Sólo configuración). Restaura los parámetros de configuración guardados anteriormente. ■ **Bootlist only** (Sólo lista de inicio). Restaura los parámetros de la lista de inicio del host guardados anteriormente por Oracle ILOM. ■ **Cancel Restore** (Cancelar restauración) (o `action=cancel`). Cancela la operación de restauración iniciada. **Nota –** La opción Cancel Restore de la interfaz web sólo está disponible si: (1) inició una operación de restauración y (2) aún no se apagó ni se reinició el sistema operativo del host en el servidor x86 gestionado de Oracle. Para obtener instrucciones sobre cómo restaurar la configuración del BIOS, consulte "Restauración de la configuración del BIOS " en la página 235.

TABLA 72 Propiedades de web y CLI del BIOS *(Continuación)*

Nombre de la propiedad	Tipo	Valores	Descripción
Transfer Method Options (Opciones de métodos de transferencia)	Lectura|Escritura	Browser | TFTP| FTP |SFTP |SCP |HTTP |HTTPS	Al importar o exportar los parámetros de configuración del BIOS de Oracle ILOM, puede especificar uno de los siguientes métodos de transferencia: ■ **Browser** (Explorador). Opción de la interfaz web únicamente. Esta opción permite especificar la ubicación del archivo. ■ **TFTP**. Esta opción permite especificar la dirección IP o el nombre del host de TFTP y la ruta del directorio del archivo. ■ **FTP**. Esta opción permite especificar la dirección IP o el nombre del host, el nombre de usuario y la contraseña del servidor FTP, además de la ruta del directorio correspondiente a la ubicación del archivo. ■ **SFTP**. Esta opción permite especificar la dirección IP o el nombre del host, el nombre de usuario y la contraseña del servidor SFTP, además de la ruta del directorio correspondiente a la ubicación del archivo. ■ **SCP**. Esta opción permite especificar la dirección de red del host, el nombre de usuario y la contraseña del servidor SCP, además de la ruta del directorio correspondiente a la ubicación del archivo. ■ **HTTP**. Esta opción permite especificar la dirección de red del host, el nombre de usuario y la contraseña del servidor HTTP, además de la ruta del directorio correspondiente a la ubicación del archivo. ■ **HTTPS**. Esta opción permite especificar la dirección IP o el nombre de red del host, el nombre de usuario y la contraseña del servidor HTTPS, además de la ruta del directorio correspondiente a la ubicación del archivo.

TABLA 73 Opción `-force` para los comandos de CLI `load` y `dump`

`load_uri=-force` *restore_option*`/`*transfer_method*`://`*username:password*`@`*ipaddress_or_hostname* `/`*directorypath*`/`*filename*

TABLA 73 Opción -force para los comandos de CLI load y dump (Continuación)

dump_uri=-force *transfer_method*://*username*:*password*@*ipaddress_or_hostname* /*directorypath*/*filename*
Uso. Debe especificar la opción -force para evitar errores en los comandos load o dump cuando: (1) aparece el estado "Pending Restore" (Restauración pendiente) para Restore Status (Estado de restauración) (restore_status=pending_restore) o (2) cuando aparece el estado "Reboot Needed" (Reinicio necesario) para BIOS Configuration Sync (Sincronización de configuración del BIOS) (config_sync_status=reboot_needed).
Precaución – Se copia una versión no sincronizada del archivo de configuración del BIOS del host en el sistema de archivos de Oracle ILOM cuando: (1) aparece el estado "Reboot Needed" (Reinicio necesario) para BIOS Configuration Sync (Sincronización de configuración del BIOS) (sync_status=reboot_needed) y (2) se utiliza la opción dump_uri=-force para realizar una copia de seguridad del archivo de configuración del BIOS.
Precaución – Los parámetros de un archivo de configuración existente del BIOS con restauración pendiente se reemplazan por los parámetros del último archivo de configuración del BIOS con copia de seguridad cuando: (1) aparece el estado "Restore Pending" (Restauración pendiente) para Restore Status (Estado de restauración) (restore_status=restore_pending) y (2) se utiliza la opción load_uri=-force para restaurar los parámetros del almacén de datos no volátiles del BIOS del host.

Realización de tareas de configuración del BIOS desde Oracle ILOM

- "Requisitos para las tareas de configuración del BIOS" en la página 229
- "Visualización del estado de sincronización de la configuración del BIOS y sincronización de los parámetros de configuración" en la página 231
- "Restablecimiento de los valores predeterminados de fábrica para el SP y el BIOS de Oracle ILOM" en la página 232
- "Copia de seguridad de la configuración del BIOS " en la página 234
- "Restauración de la configuración del BIOS " en la página 235

Requisitos para las tareas de configuración del BIOS

Antes de llevar a cabo una operación de copia de seguridad o restauración de los parámetros de configuración del BIOS, se deben cumplir los siguientes requisitos:

- Se necesitan los siguientes roles de usuario en Oracle ILOM para la sincronización, restauración o copia de seguridad de los parámetros de configuración del BIOS:

Tarea de configuración del BIOS	Roles de usuario de Oracle ILOM	Descripción:
Restaurar la configuración del BIOS (`load_uri=`)	Reset and Host Control (r) Admin (a)	Se necesitan los roles Reset and Host Control (Restablecimiento y control del host) (r) y Admin (Administrador) (a) para cargar los parámetros de configuración en el almacén de datos no volátiles del BIOS del host. **Nota –** Oracle ILOM reemplaza los parámetros del almacén de datos no volátiles del BIOS del host por los parámetros definidos por última vez en el archivo de configuración del BIOS de Oracle ILOM.
Realizar una copia de seguridad de la configuración del BIOS (`dump_uri=`)	Reset and Host Control (r) Admin (a)	Se necesitan los roles Reset and Host Control (Restablecimiento y control del host) (r) y Admin (Administrador) (a) para reemplazar los parámetros de configuración en el archivo de configuración de Oracle ILOM. **Nota –** Oracle ILOM reemplaza los parámetros del archivo de configuración de Oracle ILOM por los parámetros definidos por última vez en el almacén de datos no volátiles del BIOS del host.
Sincronizar la configuración del BIOS (`reset /System` o `stop /System`)	Admin (a)	Se necesita el rol Admin (Administrador) (a) para reiniciar (o apagar) el servidor x86 gestionado de Oracle.

- Consulte "Web y CLI: propiedades del BIOS" en la página 223 antes de llevar a cabo las tareas de configuración del BIOS documentadas en esta sección.
- Si el servidor x86 gestionado de Oracle es nuevo, se debe encender para permitir que el proceso de inicio del BIOS del host detecte los dispositivos de inicio, cree un orden de inicio y guarde esos parámetros en el almacén de datos no volátiles del BIOS. Posteriormente, se debe apagar y volver a encender el servidor x86 gestionado de Oracle a fin de sincronizar el almacén de datos no volátiles del BIOS con el archivo de configuración del BIOS de Oracle ILOM.
- Si se establecen los valores predeterminados de fábrica para `/SP` o para `/System/BIOS`, estos comandos pueden verse afectados accidentalmente. Por ejemplo, si se establece `/SP/reset_to_defaults` en *factory*, es posible que Oracle ILOM pierda la configuración de `/System/BIOS/reset_to_defaults`. Para obtener instrucciones sobre cómo establecer los valores predeterminados de fábrica para la configuración del SP y del BIOS, siga los pasos que se describen en "Restablecimiento de los valores predeterminados de fábrica para el SP y el BIOS de Oracle ILOM" en la página 232.

▼ Visualización del estado de sincronización de la configuración del BIOS y sincronización de los parámetros de configuración

Antes de empezar

- Consulte "Requisitos para las tareas de configuración del BIOS" en la página 229.

Siga estos pasos para ver el estado de sincronización de la configuración del BIOS y, si es necesario, sincronizar los parámetros de configuración del BIOS del almacén de datos no volátiles del host con los parámetros del archivo de configuración del BIOS de Oracle ILOM.

1 Para ver el estado de los parámetros definidos actualmente en el archivo de configuración del BIOS de Oracle ILOM, siga estos pasos:

- Para la interfaz web, haga clic en System Management (Gestión del sistema) > BIOS.
- Para la CLI, escriba: **`show /System/BIOS/Config`**

El estado `OK` indica que los parámetros del archivo de configuración del BIOS de Oracle ILOM están sincronizados con el almacén de datos no volátiles del BIOS.

El estado `Reboot_Required` indica que el archivo de configuración del BIOS de Oracle ILOM no está sincronizado con el almacén de datos no volátiles del BIOS.

El estado `Internal_Error` indica que Oracle ILOM no puede leer el almacén de datos no volátiles del BIOS. Este error interno impide que se inicien las operaciones de copia de seguridad y restauración de la configuración del BIOS en Oracle ILOM. Para obtener más ayuda, póngase en contacto con el servicio de asistencia de Oracle.

2 Si desea sincronizar los parámetros del almacén de datos no volátiles del BIOS con el archivo de configuración del BIOS de Oracle ILOM, realice una de las siguientes acciones para apagar y volver a encender el servidor x86 gestionado de Sun.

- En la interfaz web, haga clic en Host Management (Gestión de hosts) > Power Control (Control de energía) > Power Cycle (Apagado y encendido).
- En la CLI, escriba: **`reset /System`**

Oracle ILOM recupera los parámetros definidos en el almacén de datos no volátiles del BIOS, los guarda en el archivo de configuración del BIOS de Oracle ILOM y actualiza el estado de sincronización de la configuración.

Más información

Información relacionada:

- "Restablecimiento de la configuración del BIOS a los valores predeterminados de fábrica " en la página 232

- “Restablecimiento de los valores predeterminados de fábrica para el SP y el BIOS de Oracle ILOM” en la página 232
- “Copia de seguridad de la configuración del BIOS ” en la página 234
- “Restauración de la configuración del BIOS ” en la página 235

▼ Restablecimiento de la configuración del BIOS a los valores predeterminados de fábrica

Antes de empezar

- Consulte “Requisitos para las tareas de configuración del BIOS” en la página 229.

● **Realice una de las siguientes acciones para restablecer los parámetros del almacén de datos no volátiles del BIOS a los valores predeterminados de fábrica:**

- En la interfaz web, haga clic en System Management (Gestión del sistema) > BIOS, seleccione Factory (Fábrica) en el cuadro de lista Reset To Defaults (Restablecer valores predeterminados) y haga clic en Save (Guardar).
- En la CLI, escriba: **`set /System/BIOS reset_to_defaults=factory`**

Oracle ILOM restablece los parámetros de configuración del BIOS del almacén de datos no volátiles a los valores predeterminados de fábrica. El valor Reset To Defaults (Restablecer valores predeterminados) se restablece en None (Ninguno) una vez aplicados los parámetros predeterminados de fábrica.

Más información Información relacionada:

- “Visualización del estado de sincronización de la configuración del BIOS y sincronización de los parámetros de configuración” en la página 231
- “Restablecimiento de los valores predeterminados de fábrica para el SP y el BIOS de Oracle ILOM” en la página 232
- “Copia de seguridad de la configuración del BIOS ” en la página 234
- “Restauración de la configuración del BIOS ” en la página 235

▼ Restablecimiento de los valores predeterminados de fábrica para el SP y el BIOS de Oracle ILOM

Antes de empezar

- Consulte “Requisitos para las tareas de configuración del BIOS” en la página 229.

Siga estos pasos para restablecer la configuración de Oracle ILOM y la configuración del BIOS del host a los valores predeterminados de fábrica desde la CLI o la interfaz web de Oracle ILOM.

1 Apague el sistema operativo del host en el servidor x86 gestionado de Oracle. Para ello, siga uno de estos pasos:

- En la interfaz web, haga clic en Host Management (Gestión de hosts) > Power Control (Control de energía) > Power Cycle (Apagado y encendido).
- En la CLI, escriba: **`stop -force /System`**

2 Restablezca los parámetros del almacén de datos no volátiles del BIOS a los valores predeterminados de fábrica. Para ello, siga uno de estos pasos:

- En la interfaz web, haga clic en System Management (Gestión del sistema) > BIOS, seleccione Factory (Fábrica) en el cuadro de lista Reset To Defaults (Restablecer valores predeterminados) y haga clic en Save (Guardar).
- En la CLI, escriba: **`set /System/BIOS reset_to_defaults=factory`**

Nota – Espere hasta que `/System/BIOS reset_to_defaults` cambie de *factory* a *none* antes de continuar con el paso 3. El valor `reset_to_default` se restablece en *none* una vez que se aplicaron los valores predeterminados de fábrica al almacén de datos no volátiles del BIOS.

---

3 Restablezca la configuración de Oracle ILOM a los valores predeterminados de fábrica. Para ello, siga uno de estos pasos:

- En la interfaz web, haga clic en ILOM Administration (Administración de ILOM) > Configuration Management (Gestión de configuración) > Reset Defaults (Restablecer valores predeterminados), seleccione Factory (Fábrica) en el cuadro de lista Reset Defaults y haga clic en Reset Defaults.
- En la CLI, escriba: **`set /SP reset_to_default=factory`**

4 Apague y vuelva a encender el SP de Oracle ILOM. Para ello, siga uno de estos pasos:

- En la interfaz web, haga clic en Host Management (Gestión de hosts) > Power Control (Control de energía) > Reset (Reinicio).
- En la CLI, escriba: **`reset /SP`**

Oracle ILOM restablece los parámetros de configuración del BIOS a los valores predeterminados de fábrica y devuelve None (Ninguno) para Sync Status (Estado de sincronización).

Más información Información relacionada:

- "Visualización del estado de sincronización de la configuración del BIOS y sincronización de los parámetros de configuración" en la página 231
- "Restablecimiento de la configuración del BIOS a los valores predeterminados de fábrica " en la página 232
- "Copia de seguridad de la configuración del BIOS " en la página 234

- "Restauración de la configuración del BIOS " en la página 235

Copia de seguridad de la configuración del BIOS

Antes de empezar

- Consulte "Requisitos para las tareas de configuración del BIOS" en la página 229.
- La operación de copia de seguridad de la configuración del BIOS normalmente tarda de dos a tres minutos en completarse.

Siga este procedimiento para realizar una copia de seguridad de los parámetros del almacén de datos no volátiles del BIOS en el archivo de configuración del BIOS de Oracle ILOM.

1. **Para realizar una copia de seguridad de la configuración del BIOS, siga uno de estos pasos:**
   - En la interfaz web, haga clic en System Management (Gestión del sistema) > BIOS y, en la sección Backup (Copia de seguridad), seleccione una opción en el cuadro de lista Transfer Method (Método de transferencia), especifique los parámetros necesarios para el método de transferencia y haga clic en Start Backup (Iniciar copia de seguridad).
   - En la CLI, escriba:

     set dump_uri *transfer_method*://*username:password*@*ipaddress_or_hostname* /*directorypath*/*filename*

     Donde:

     - aparece *transfer_method*, escriba: tftp, ftp, sftp, scp, http o https.
     - aparece *username*, escriba el nombre de la cuenta de usuario para el servidor del método de transferencia elegido. El nombre de usuario es obligatorio para scp, sftp y ftp. El nombre de usuario no es obligatorio para tftp, y es opcional para http y https.
     - aparece *password*, escriba la contraseña de la cuenta de usuario para el servidor del método de transferencia elegido. La contraseña es obligatoria para scp, sftp y ftp. La contraseña no se utiliza para tftp, y es opcional para http y https.
     - aparece *ipaddress_or_hostname*, escriba la dirección IP o el nombre de host para el servidor del método de transferencia elegido.
     - aparece *directorypath*, escriba la ubicación del almacenamiento de archivos en el servidor del método de transferencia.
     - aparece *filename*, escriba el nombre asignado a la copia de seguridad del archivo de configuración, por ejemplo: `foo.xml`.

2. **Espere hasta que Oracle ILOM complete la operación de copia de seguridad del BIOS.**

   Oracle ILOM recupera una copia del archivo de configuración del almacén de datos no volátiles del BIOS y la guarda en el sistema de archivos de Oracle ILOM.

Más información

Información relacionada:

- "Web y CLI: propiedades del BIOS" en la página 223
- Tabla 73
- "Visualización del estado de sincronización de la configuración del BIOS y sincronización de los parámetros de configuración" en la página 231
- "Restablecimiento de la configuración del BIOS a los valores predeterminados de fábrica " en la página 232
- "Restablecimiento de los valores predeterminados de fábrica para el SP y el BIOS de Oracle ILOM" en la página 232
- "Restauración de la configuración del BIOS " en la página 235

▼ Restauración de la configuración del BIOS

Antes de empezar

- Consulte "Requisitos para las tareas de configuración del BIOS" en la página 229.
- Los datos de la sección de dispositivos de inicio del archivo de configuración de Oracle ILOM son de sólo lectura y no afectan los parámetros restaurados en el almacén de datos no volátiles del BIOS.
- La operación de restauración de la configuración del BIOS normalmente tarda de dos a tres minutos en completarse.

Siga este procedimiento para restaurar los parámetros del archivo de configuración del BIOS de Oracle ILOM en el almacén de datos no volátiles del BIOS.

1 **Para restaurar la configuración del BIOS, siga uno de estos pasos:**

- En la interfaz web, haga clic en System Management (Gestión del sistema) > BIOS, seleccione una opción de restauración y una opción de método de transferencia, especifique los parámetros necesarios para el método de transferencia y haga clic en Start Restore (Iniciar restauración).
- En la CLI, escriba:

  set load_uri=*restore_option***/***transfer_method***://***username*:*password***@***ipaddress_or_hostname***/***directorypath***/***filename*

  Donde:

  - aparece *restore option*, escriba: all, config-only o bootlist-only.
  - aparece *transfer_method*, escriba: tftp, ftp, sftp, scp, http o https.
  - aparece *username*, escriba el nombre de la cuenta de usuario para el servidor del método de transferencia elegido. El nombre de usuario es obligatorio para scp, sftp y ftp. El nombre de usuario no es obligatorio para tftp, y es opcional para http y https.

- aparece *password*, escriba la contraseña de la cuenta de usuario para el servidor del método de transferencia elegido. La contraseña es obligatoria para scp, sftp y ftp. La contraseña no se utiliza para tftp, y es opcional para http y https.
- aparece *ipaddress_or_hostname*, escriba la dirección IP o el nombre de host para el servidor del método de transferencia elegido.
- aparece *directorypath*, escriba la ubicación del almacenamiento del archivo de configuración de Oracle ILOM (`/System/BIOS/Config`) en el servidor del método de transferencia.
- aparece *filename*, escriba el nombre asignado al archivo de configuración de Oracle ILOM, por ejemplo: `foo.xml`.

Nota – Para cancelar una acción de restauración de la configuración del BIOS pendiente, escriba: `set action=cancel`

---

2 Espere hasta que Oracle ILOM complete la operación de restauración.

Oracle ILOM exporta los parámetros de configuración del BIOS del archivo de configuración del BIOS de Oracle ILOM al almacén de datos no volátiles del BIOS y actualiza el estado de restauración.

3 Compruebe el estado de restauración para determinar si la operación de restauración se completó correctamente.

Para obtener una lista de las descripciones de los estados de restauración, consulte “Web y CLI: propiedades del BIOS” en la página 223.

Nota – Los resultados de la operación de restauración se guardan en el registro de eventos de Oracle ILOM (`/SP/logs/event list`).

Más información

Información relacionada

- “Web y CLI: propiedades del BIOS” en la página 223
- Tabla 73
- “Visualización del estado de sincronización de la configuración del BIOS y sincronización de los parámetros de configuración” en la página 231
- “Restablecimiento de la configuración del BIOS a los valores predeterminados de fábrica ” en la página 232
- “Restablecimiento de los valores predeterminados de fábrica para el SP y el BIOS de Oracle ILOM” en la página 232
- “Copia de seguridad de la configuración del BIOS ” en la página 234

Recursos de almacenamiento del blade del chasis de zonas SAS

Descripción	Vínculos
Consulte esta sección para obtener información sobre las opciones de gestión admitidas para dispositivos de almacenamiento en el nivel de chasis de zonas.	■ "Gestión de zonas para recursos compatibles con SAS-2 en el nivel del chasis" en la página 237
Consulte esta sección para obtener información sobre las propiedades de Sun Blade Zone Manager de Oracle ILOM.	■ "Propiedades de Sun Blade Zone Manager " en la página 239
Consulte esta sección para obtener información importante sobre cómo guardar, realizar copias de seguridad y recuperar parámetros de configuración de zonas SAS.	■ "Consideraciones importantes sobre las asignaciones de zonas SAS " en la página 248
Consulte esta sección para conocer los procedimientos para activar Sun Blade Zone Manager y crear asignaciones de zonas SAS.	■ "Activación de zonas y creación de asignaciones de zonas SAS-2" en la página 249
Consulte esta sección para conocer los procedimientos para ver y modificar asignaciones de almacenamiento existentes.	■ "Gestión de asignaciones de recursos de almacenamiento SAS-2 existentes" en la página 266
Consulte esta sección para restablecer todas las asignaciones de almacenamiento guardadas a los valores predeterminados de fábrica.	■ "Restablecimiento de asignaciones de Sun Blade Zone Manager a los valores predeterminados de fábrica" en la página 275
Consulte esta sección para restablecer, de manera opcional, la contraseña de gestión en banda.	■ "Restablecimiento de la contraseña de zona al valor predeterminado de fábrica para gestión en banda de terceros " en la página 276

Gestión de zonas para recursos compatibles con SAS-2 en el nivel del chasis

Oracle ILOM ofrece compatibilidad de gestión de zonas para dispositivos de almacenamiento SAS-2 en el nivel de chasis instalados en un sistema de chasis Sun Blade. Puede elegir gestionar

el acceso a los recursos de almacenamiento en el nivel de chasis Sun Blade mediante el uso de Sun Blade Zone Manager de Oracle ILOM o una aplicación en banda de terceros. Para obtener más información, consulte:

- "Gestión de zonas mediante una aplicación de gestión en banda de terceros" en la página 238
- "Gestión de zonas mediante Sun Blade Zone Manager de Oracle ILOM" en la página 238
- "Dispositivos compatibles con zonas SAS-2 gestionables" en la página 239

Gestión de zonas mediante una aplicación de gestión en banda de terceros

Si su entorno admite la gestión de acceso a dispositivos de almacenamiento en el nivel de chasis mediante una aplicación de gestión en banda de terceros, debe verificar que el estado de Sun Blade Zone Manager en Oracle ILOM esté desactivado (predeterminado). Si necesita restablecer la contraseña de gestión en banda a los valores predeterminados de fábrica, puede hacerlo en Oracle ILOM. Para obtener instrucciones, consulte "Restablecimiento de la contraseña de zona al valor predeterminado de fábrica para gestión en banda de terceros " en la página 276.

Gestión de zonas mediante Sun Blade Zone Manager de Oracle ILOM

Cuando Sun Blade Zone Manager está activado en el CMM de Oracle ILOM, puede gestionar permisos de almacenamiento SAS-2 en el nivel de chasis para los servidores CPU Sun Blade instalados en el chasis. Para obtener más información acerca del uso de Sun Blade Zone Manager de Oracle ILOM, consulte estos temas:

- "Dispositivos compatibles con zonas SAS-2 gestionables" en la página 239
- "Propiedades de Sun Blade Zone Manager " en la página 239
- "Consideraciones importantes sobre las asignaciones de zonas SAS " en la página 248
- "Activación de zonas y creación de asignaciones de zonas SAS-2" en la página 249
- "Gestión de asignaciones de recursos de almacenamiento SAS-2 existentes" en la página 266
- "Restablecimiento de asignaciones de Sun Blade Zone Manager a los valores predeterminados de fábrica" en la página 275

Dispositivos compatibles con zonas SAS-2 gestionables

El CMM de Oracle ILOM reconoce los siguientes dispositivos en un sistema de chasis Sun Blade como dispositivos compatibles con zonas SAS-2 gestionables:

- Servidor de CPU Sun Blade con módulos de expansión RAID (REM) SAS-2
- Módulos de ampliación de red (NEM) de sistema de chasis Sun Blade
- Servidor de almacenamiento Sun Blade (por ejemplo, Sun Blade Storage Module M2)

Nota – Oracle ILOM no admite la gestión de zonas para: (1) módulos de almacenamiento internos instalados en un servidor de CPU Sun Blade; (2) Módulos de expansión de tejido (FMOD) en un blade de almacenamiento Sun; o (3) recursos de almacenamiento SAS-2 de red externos conectados a un sistema de chasis Sun Blade mediante los puertos SAS-2 externos de un NEM.

Nota – La CLI de Sun Blade Zone Manager no reconocerá ni enumerará la presencia de dispositivos de almacenamiento SAS-2 no compatibles y no gestionables. No obstante, en algunos casos, la interfaz web de Sun Blade Zone Manager puede reconocer y enumerar la presencia de dispositivos de almacenamiento SAS-2 no compatibles y no gestionables. En estos casos, los dispositivos de almacenamiento que no son SAS-2 en la interfaz web de Sun Blade Zone Manager se etiquetan como recursos que no son SAS-2.

Propiedades de Sun Blade Zone Manager

Oracle ILOM ofrece un conjunto de propiedades fáciles de usar para configurar y gestionar permisos de acceso a los dispositivos de almacenamiento SAS-2 en el nivel de chasis. Para obtener más información, consulte:

- "Web de Sun Blade Zone Manager: Propiedades" en la página 239
- "CLI de Sun Blade Zone Manager: Destinos y propiedades" en la página 246

Web de Sun Blade Zone Manager: Propiedades

Se puede acceder a la página Sun Blade Zone Manager Settings (Configuración de Sun Blade Zone Manager) desde la interfaz web del CMM de Oracle ILOM haciendo clic en System Management (Gestión del sistema) > SAS Zoning (Zonas SAS). La página Sun Blade Zone Manager Settings ofrece las siguientes opciones para activar, configurar y gestionar permisos de zonas SAS:

- "Sun Blade Zone Manager: Estado" en la página 240
- "Whole Chassis Setup: Quick Setup (Configuración de todo el chasis: Configuración rápida)" en la página 240

- “Full Resource Control: Detailed Setup (Control total de recursos: Configuración detallada)” en la página 245
- “Zoning Reset: Reset All (Restablecimiento de zona: Restablecer todo) ” en la página 246

Sun Blade Zone Manager: Estado

El estado de Sun Blade Zone Manager en la interfaz web del CMM de Oracle ILOM se muestra en la página Sun Blade Zone Manager Settings (Configuración de Sun Blade Zone Manager).

Cuando el estado está activado, Sun Blade Zone Manager ofrece capacidades de zona basadas en plantilla (Configuración rápida) o personalizadas (Configuración detallada) para los dispositivos de almacenamiento SAS-2 instalados en el chasis.

Cuando el estado está desactivado (opción predeterminada), Oracle ILOM puede gestionar los permisos de acceso a los dispositivos de almacenamiento SAS-2 instalados en el chasis y las opciones de Quick Setup (Configuración rápida) y Detailed Setup (Configuración detallada) están ocultas en la página Sun Blade Zone Manager Settings.

Para obtener instrucciones sobre cómo activar el estado de Sun Blade Zone Manager, consulte “Acceso y activación de Sun Blade Zone Manager ” en la página 250.

Whole Chassis Setup: Quick Setup (Configuración de todo el chasis: Configuración rápida)

La función Whole Chassis Setup de la interfaz web generalmente se utiliza al configurar el acceso a zonas por primera vez para todos los dispositivos de almacenamiento SAS-2 en el nivel de chasis. Esta función ofrece las siguientes opciones de zona de Quick Setup:

- “Opción 1: Assign to Individual Disks (Asignar a discos individuales) (Quick Setup [Configuración rápida])” en la página 240
- “Opción 2: Assign to Adjacent Individual Disks (Asignar a discos adyacentes individuales) (Quick Setup [Configuración rápida])” en la página 241
- “Opción 3: Assign to Individual Storage Blade (Asignar a blade de almacenamiento individual) (Quick Setup [Configuración rápida])” en la página 242
- “Opción 4: Assign to Adjacent Storage Blade (Asignar a blade de almacenamiento adyacente) (Quick Setup [Configuración rápida]) ” en la página 243

Opción 1: Assign to Individual Disks (Asignar a discos individuales) (Quick Setup [Configuración rápida])

La primera opción de zona, que se muestra en el diálogo Quick Setup, utiliza un algoritmo round-robin para asignar uniformemente la propiedad de almacenamiento en todos los servidores blade de CPU del chasis.

La opción 1 es ideal para la operación del sistema de chasis tolerante a fallos cuando el error o la eliminación de un servidor blade de almacenamiento único no desactivará todos los arreglos de almacenamiento.



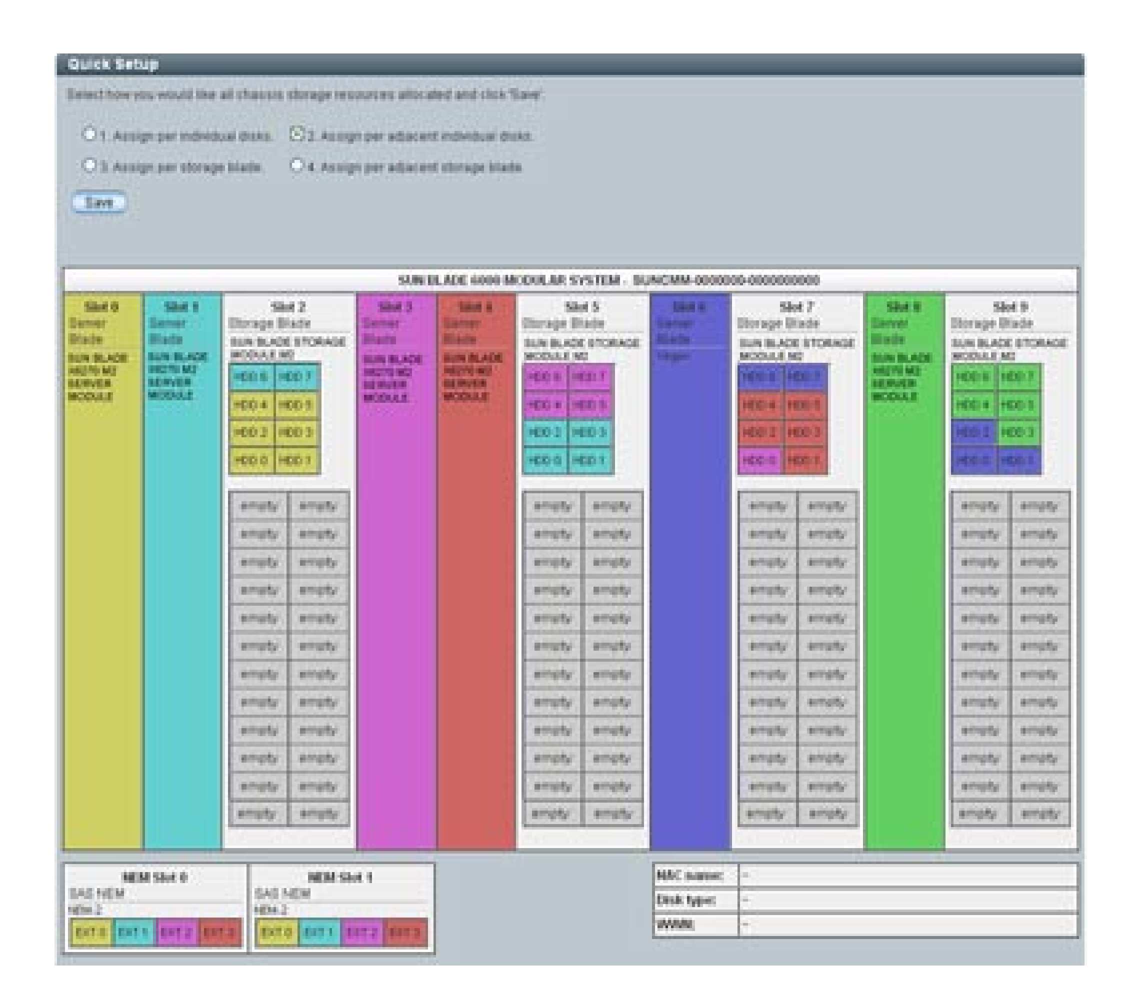
Nota – Las ranuras vacías que se muestran en el diálogo Quick Setup representan las ranuras del blade del chasis que están vacías (no tienen nada instalado).

Opción 2: Assign to Adjacent Individual Disks (Asignar a discos adyacentes individuales) (Quick Setup [Configuración rápida])

La segunda opción de asignación de zona, que se muestra en el diálogo Quick Setup, divide equitativamente la cantidad de discos de almacenamiento de blade entre los servidores blade de CPU adyacentes.

La opción 2 intenta asignar la misma cantidad de discos de almacenamiento posible a cada servidor blade de CPU adyacente. Si no existen blades de almacenamiento adyacentes a un blade de CPU, Sun Blade Zone Manager asignará discos de almacenamiento del blade de almacenamiento más cercano posible.

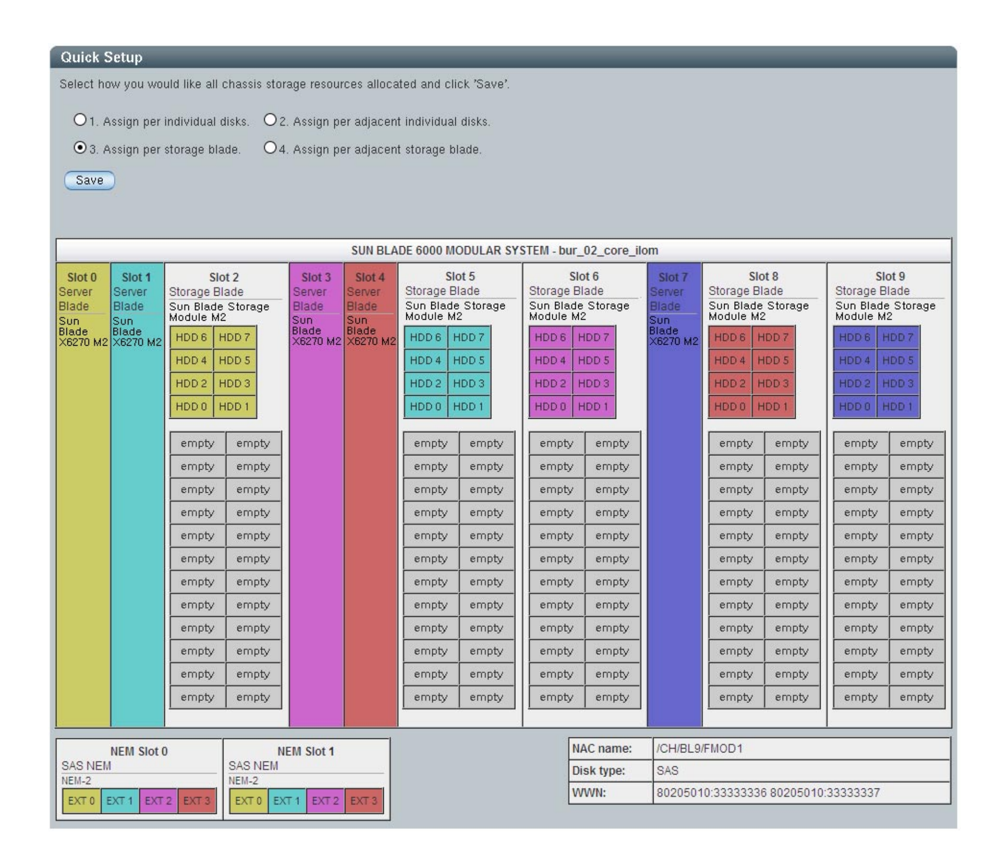
La asignación de blades de CPU a discos de almacenamiento adyacentes es ideal para cuando: 1) el sistema de chasis Sun Blade contenga más servidores blade de CPU que los servidores blade de almacenamiento y 2) desea implementar equitativamente los recursos de almacenamiento entre cada servidor blade de CPU.



Opción 3: Assign to Individual Storage Blade (Asignar a blade de almacenamiento individual) (Quick Setup [Configuración rápida])

La tercera opción de asignación de zona, que se muestra en el diálogo Quick Setup, analiza el sistema de chasis Sun Blade en busca de servidores blade de CPU (a partir de la ranura 0) y luego asigna los discos de almacenamiento desde el blade de almacenamiento más cercano disponible.

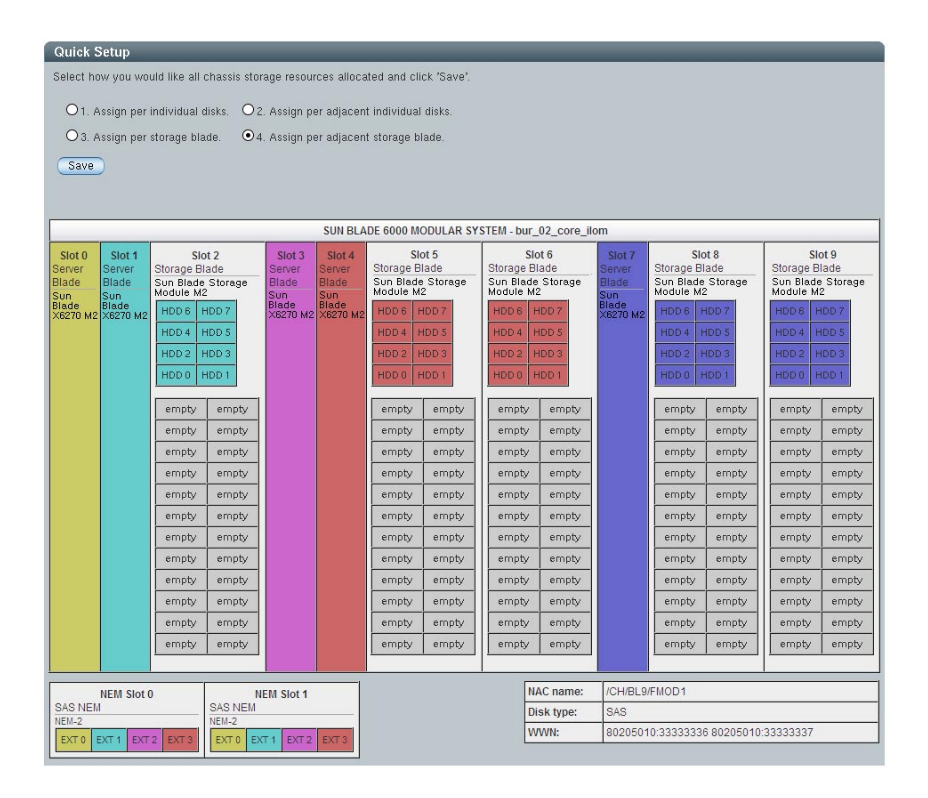
La opción 3 es ideal para sistemas de chasis que contienen una cantidad igual de servidores blade de almacenamiento y servidores blade de CPU o en los casos en que existen más servidores blade de almacenamiento que servidores blade de CPU. De lo contrario, si hay menos servidores blade de almacenamiento que servidores blade de CPU en el chasis, Sun Blade Zone Manager no podrá asignar almacenamiento a algunos servidores blade de CPU.



Opción 4: Assign to Adjacent Storage Blade (Asignar a blade de almacenamiento adyacente) (Quick Setup [Configuración rápida])

La cuarta opción de asignación de zona, que se muestra en el diálogo Quick Setup, analiza el sistema de chasis Sun Blade en busca de servidores blade de CPU en una ranura adyacente. Si el servidor blade de CPU no tiene un servidor blade de almacenamiento en una ranura de chasis adyacente, Sun Blade Zone Manager no asignará almacenamiento a dicho servidor blade de CPU.

La opción 4 es ideal para sistemas de chasis que contengan: (1) un número igual de servidores blade de almacenamiento y servidores blade de CPU y (2) en los casos en que el servidor blade de CPU esté instalado en una ranura de chasis que esté adyacente a un servidor blade de almacenamiento.



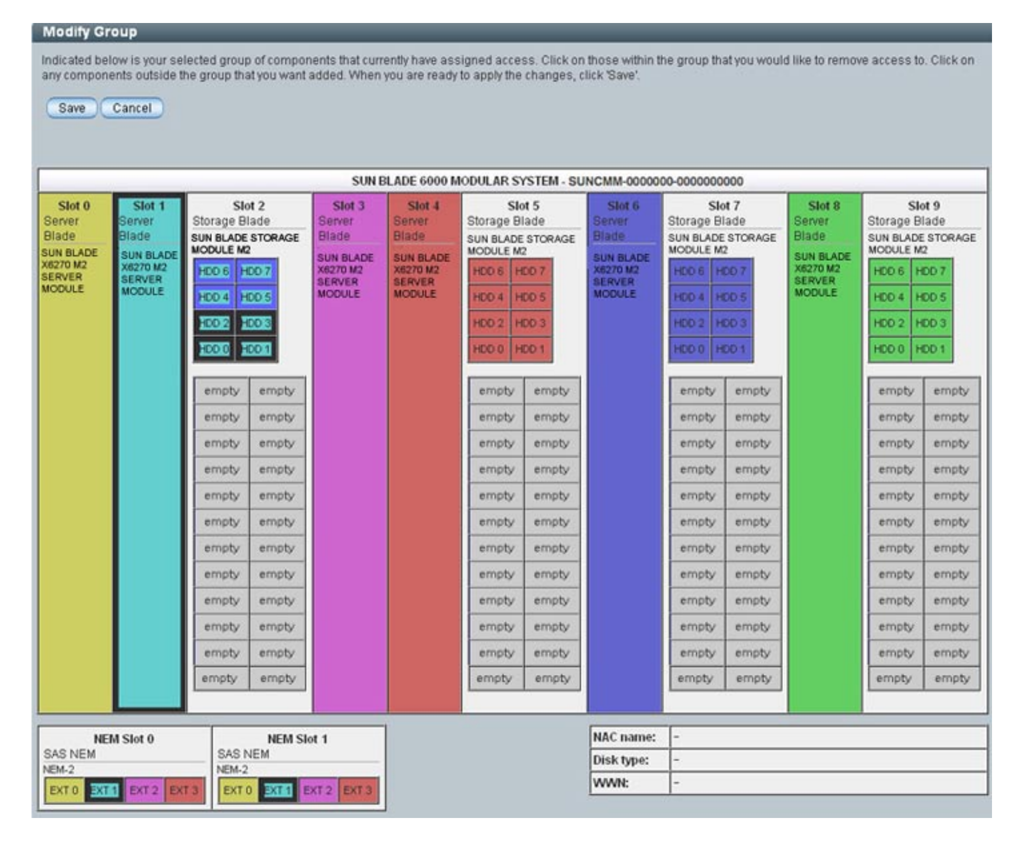
Nota – Los destinos NEM0 y NEM1 se muestran en Zone Manager cuando se instalan estos NEM; sin embargo, las conexiones externas de NEM a dispositivos de almacenamiento de red SAS-2 no se admiten o no se muestran en Sun Blade Zone Manager.

Para obtener más instrucciones sobre cómo crear asignaciones de zonas SAS para todo el chasis, consulte "Asignación de almacenamiento a todo el chasis: Quick Setup (Configuración rápida) (Web)" en la página 252.

Full Resource Control: Detailed Setup (Control total de recursos: Configuración detallada)

La opción Full Resource Control: Detailed Setup de la interfaz web le permite crear nuevas asignaciones a recursos de almacenamiento o cambiar las asignaciones de recursos de almacenamiento existentes. Por ejemplo, al usar la opción Full Resource Control: Detailed Setup, puede elegir:

- Agregar asignaciones de almacenamiento a un servidor blade de CPU haciendo clic en los componentes fuera del grupo de servidores codificados con color.
- Eliminar asignaciones de recursos de almacenamiento asignados a un servidor blade de CPU haciendo clic en los componentes dentro del grupo de servidores codificados con color.
- Compartir una asignación de recursos única entre uno o varios servidores blade de CPU.



Para obtener más instrucciones para usar la opción Detailed Setup para crear o cambiar asignaciones de recursos, consulte:

- “Asignación de recursos de almacenamiento a un servidor blade único: Detailed Setup (Configuración detallada) (Web)” en la página 254
- “Asignación de recurso de almacenamiento único a varios servidores blade: Detailed Setup (Configuración detallada) (Web)” en la página 260
- “Modificación de asignaciones de grupos de blade existentes (Web)” en la página 269

Zoning Reset: Reset All (Restablecimiento de zona: Restablecer todo)

Cuando el estado de Sun Blade Zone Manager está activado, la opción para restablecer la configuración de zona a los valores predeterminados de fábrica se muestra en la página Sun Blade Zone Manager Settings (Configuración de Sun Blade Zone Manager) (System Management [Gestión del sistema] > SAS Zoning [Zonas SAS]).

Para obtener instrucciones para restablecer los parámetros de Sun Blade Zone Manager a los valores predeterminados de fábrica, consulte “Restablecimiento de las asignaciones de zona a los valores predeterminados de fábrica (Web) ” en la página 275.

CLI de Sun Blade Zone Manager: Destinos y propiedades

La CLI del CMM de Oracle ILOM proporciona acceso a los destinos y propiedades de zonas en el espacio de nombres `/STORAGE/sas_zoning`.

Propiedades de zonas SAS	Valores	Valor predeterminado	Descripción
`zone_management_state=`	*disabled |enabled*	Disabled (desactivado)	Cuando se establece en Disabled, Sun Blade Zone Manager no puede gestionar los recursos de almacenamiento de chasis SAS-2. Cuando se establece en Enabled (Activado), Sun Blade Zone Manager ofrece capacidades de zona basadas en plantillas o personalizadas para los recursos SAS-2 instalados en el chasis.
`reset_password_action=`	*true*		Cuando se establece en true, la contraseña de zona de gestión en banda del CMM se establece en los valores predeterminados de fábrica (todos ceros).
`reset_access_action=`	*true*		Cuando se establece en true, los parámetros de asignación de recursos de almacenamiento actualmente guardados en el CMM se establecen en los valores predeterminados de fábrica.

Cuando se activa la zona, los blades y los NEM compatibles con SAS-2 se muestran como destinos de la CLI en `/STORAGE/sas_zoning`. Por ejemplo:

```
-> show /STORAGE/sas_zoning

     Targets
       BL0
       BL6
       BL7
       BL8
       BL9
       NEM0
       NEM1

    Properties
      zone_management_state = enabled
      reset_password_action = (Cannot show property)
      reset_access_action = (Cannot show property)

    Commands:
       cd
       set
       show
```

Nota – Los destinos NEM0 y NEM1 se muestran en Zone Manager cuando se instalan estos NEM; sin embargo, las conexiones SAS externas de Sun Blade Zone Manager no se admiten en este momento.

Los dispositivos de almacenamiento compatibles con SAS-2 en un servidor blade se muestran como destinos en `sas_zoning/BL`*n*. Por ejemplo:

```
-> show /STORAGE/sas_zoning/BL9

  Targets:
    HDD0
    HDD2
    HDD3
    HDD5
```

Las propiedades de zonas SAS disponibles en el destino de blade (BL*n*) o en el destino de dispositivo de almacenamiento (HDD*n*) incluyen:

Propiedades de blade y almacenamiento	Destino de zonas SAS	Descripción
`add_storage_access=`	/BL*n*	Utilice la propiedad `add_storage_access=` *en el destino /sas_zoning/BLn* para asignar almacenamiento a un servidor blade de CPU.
`remove_storage_access=`	/BL*n*	Utilice la propiedad `remove_storage_access=` en el destino `/sas_zoning/BL`*n* para eliminar almacenamiento de un servidor blade de CPU.

Propiedades de blade y almacenamiento	Destino de zonas SAS	Descripción
`add_host_access=`	/BL*n*/HDD*n*	Utilice la propiedad `add_host_access=` en el destino `/sas_zoning/BLn/HDDn` para asignar almacenamiento a un servidor blade de CPU.
`remove_host_access=`	/BL*n*/HDD*n*	Utilice la propiedad `remove_host_access=` en el destino `/sas_zoning/BLn/HDDn` para eliminar almacenamiento de un servidor blade de CPU.

Para obtener más instrucciones sobre cómo gestionar asignaciones de recursos de almacenamiento desde la CLI de Oracle ILOM, consulte:

- "Creación manual de asignaciones de zona SAS-2 (CLI)" en la página 264
- "Visualización y modificación de asignaciones de almacenamiento existentes (CLI)" en la página 273
- "Restablecimiento de las asignaciones de zona a los valores predeterminados de fábrica (CLI)" en la página 276
- "Restablecimiento de la contraseña de zonas (CLI)" en la página 277

Consideraciones importantes sobre las asignaciones de zonas SAS

- "Guardado de asignaciones de almacenamiento" en la página 248
- "Copia de seguridad y recuperación de asignaciones de zonas SAS-2" en la página 249

Guardado de asignaciones de almacenamiento

Cuando guarde asignaciones de almacenamiento en un blade, tenga en cuenta las siguientes consideraciones:

- Las asignaciones de almacenamiento guardadas en Oracle ILOM se basan en el hardware actualmente instalado en el chasis (blades de almacenamiento o NEM SAS-2) Si se realizan cambios en la configuración de hardware del chasis, se puede perder un grupo de blades de almacenamiento. Por lo tanto, debe realizar una copia de seguridad de todas las asignaciones de almacenamiento de chasis en Oracle ILOM. Para obtener más información, consulte "Copia de seguridad y recuperación de asignaciones de zonas SAS-2" en la página 249.

Nota – La conexión en macha de componentes de chasis, como NEM y blades de almacenamiento, también puede afectar las asignaciones de grupos de blades de almacenamiento. Para obtener más información sobre los efectos de la conexión en marcha de NEM y blades de almacenamiento, consulte la documentación de hardware de NEM o blades de almacenamiento Sun de Oracle.

- El diálogo de Sun Blade Zone Manager (Modify Group [Modificar grupo] o New Assignments [Nuevas asignaciones]) debe permanecer abierto durante toda la operación de guardado. Si se cierra el diálogo de Sun Blade Zone Manager cuando la operación de guardado está en curso, sólo se conservará una parte del grupo de blades de almacenamiento.
- No elimine ni apague y encienda ninguno de los componentes de hardware de chasis que forman parte de un grupo de blades de almacenamiento mientras la operación de guardado está en curso. Si lo hace, la asignación de grupos no se guardará correctamente.

Copia de seguridad y recuperación de asignaciones de zonas SAS-2

Oracle ILOM ofrece operaciones de copia de seguridad y restauración que le permiten: (1) crear una copia de seguridad de todos los parámetros guardados en el archivo de configuración de Oracle ILOM y (2) restaurar una copia de seguridad del archivo de configuración de Oracle ILOM. Para obtener más información sobre cómo crear una copia de seguridad y restaurar una copia de seguridad del archivo de configuración de Oracle ILOM, consulte “Recursos de almacenamiento del blade del chasis de zonas SAS ” en la página 237.

Activación de zonas y creación de asignaciones de zonas SAS-2

Requisitos del hardware del chasis

- Se debe contar con un midplane compatible con PCIe 2.0 en el chasis Sun Blade 6000. Para obtener más información sobre cómo determinar esto, consulte *Notas de producto sobre el sistema modular Sun Blade 6000*.
- La versión de software 3.2.1 o superior debe estar instalada en el CMM. Esta versión incluye la versión mínima de firmware del CMM de Oracle ILOM (3.0.10.15a), que admite SAS-2 e incluye Sun Blade Zone Manager.
- Todos los dispositivos de almacenamiento SAS-2 (módulo de servidor blade con REM SAS-2, NEM SAS-2 y módulos de almacenamiento SAS-2) deben estar debidamente instalados y encendidos en el sistema de chasis Sun Blade.

Nota – Si el estado de un dispositivo de almacenamiento SAS-2 tiene un estado con error, es posible que Sun Blade Zone Manager no pueda reconocer dicho dispositivo. Para obtener más información sobre cómo identificar y resolver errores de hardware mediante Oracle ILOM, consulte .

- Los NEM SAS-2 deben tener un nivel de versión de firmware que admita las zonas. Verifique las notas de producto de NEM para obtener la información de versión y actualizaciones disponibles.
- Se debe haber completado la configuración inicial del CMM de Oracle ILOM. Para obtener información sobre cómo establecer una conexión de gestión al CMM de Oracle ILOM, consulte “Configuración de una conexión de gestión a Oracle ILOM e inicio de sesión” en la página 11.

▼ Acceso y activación de Sun Blade Zone Manager

Antes de empezar

Cuando está activado, Sun Blade Zone Manager en Oracle ILOM ofrece una forma de limitar los servidores blade de CPU dentro de un dominio SAS que tienen acceso a los recursos de almacenamiento (HDD, FMOD, puertos SAS externos).

Antes de empezar

- Se requiere el rol Admin (a) en Oracle ILOM para modificar las propiedades de zonas SAS.
- Revise “Requisitos del hardware del chasis” en la página 250.
- Revise “Consideraciones importantes sobre las asignaciones de zonas SAS ” en la página 248.

Nota – Los blades de almacenamiento de chasis presentes en la interfaz web de Oracle ILOM no se muestran en el menú Manage (Gestionar) del CMM. Los discos de almacenamiento instalados en los servidores blade de almacenamiento se pueden visualizar desde la página System Information (Información del sistema) > Storage (Almacenamiento). Las asignaciones de recursos de blade de almacenamiento de Sun se pueden gestionar desde la página System Management (Gestión del sistema) > SAS Zoning (Zonas SAS) > Sun Blade Zone Manager Settings (Configuración de Sun Blade Zone Manager).

---

1 **Para acceder y activar Sun Blade Zone Manager desde la interfaz web del CMM, realice estos pasos:**

a. **Haga clic en System Management > SAS Zoning.**

Aparecerá la página Sun Blade Zone Manager Settings.

b. **Seleccione la casilla de verificación Enabled (Activado) y haga clic en Save (Guardar) para activar las zonas SAS.**

Después de activar Sun Blade Zone Manager, puede crear, ver y gestionar los valores de configuración de zonas SAS-2 mediante las interfaces de Oracle ILOM.

Si los servicios del CMM de Oracle ILOM aún se están inicializando, puede aparecer el siguiente mensaje:

```
Sun Blade Zone Manager Not Ready
The Sun Blade Zone Manager is initializing and not ready for operation. Please wait several minutes and then refr
```

Si aparece el mensaje mencionado, espere cinco minutos y vuelva a intentarlo. Deberá cerrar y volver a abrir, o actualizar la página de la interfaz web.

2 **Para activar la propiedad de zonas SAS desde la CLI del CMM, escriba:**

`set /STORAGE/SAS_zoning zone_management_state=enabled`

- **Aparece el siguiente mensaje.**

  ```
  Enabling the Sun Blade Zone Manager will result in the clearing of all zoning
  configuration in the installed chassis SAS hardware, and any SAS disk I/O in
  progress will be interrupted. (Si activa Sun Blade Zone Manager, se borrarán
  todas las configuraciones de zonas del hardware SAS instalado y se
  interrumpirán todos los discos I/O [E/S] SAS en progreso.)
  ```

  ```
  Are you sure you want to enable the Sun Blade Zone Manager (y/n)? (¿Está
  seguro de que desea activar Sun Blade Zone Manager [s/n]?)
  ```

- **Para continuar, escriba: y**

  Aparece el siguiente mensaje.

```
Set ?zone_management_state? to ?enabled? (Establecer ?zone_management_state?
en activado)
```

- **Si el CMM de Oracle ILOM no puede inicializar Sun Blade Zone Manager, aparece el siguiente mensaje:**

  ```
  set: The Sun Blade Zone Manager is initializing and not ready for operation
  (Sun Blade Zone Manager se está inicializando y todavía no está listo para
  funcionar). Please wait several minutes and try again. (Espere unos minutos y
  vuelva a intentarlo)
  ```

  Si aparece el mensaje mencionado, espere cinco minutos y vuelva a intentar el comando.

Más información

Información relacionada

- "Asignación de almacenamiento a todo el chasis: Quick Setup (Configuración rápida) (Web)" en la página 252
- "Asignación de recursos de almacenamiento a un servidor blade único: Detailed Setup (Configuración detallada) (Web)" en la página 254
- "Creación manual de asignaciones de zona SAS-2 (CLI)" en la página 264
- "Gestión de asignaciones de recursos de almacenamiento SAS-2 existentes" en la página 266
- "Restablecimiento de asignaciones de Sun Blade Zone Manager a los valores predeterminados de fábrica" en la página 275

▼ Asignación de almacenamiento a todo el chasis: Quick Setup (Configuración rápida) (Web)

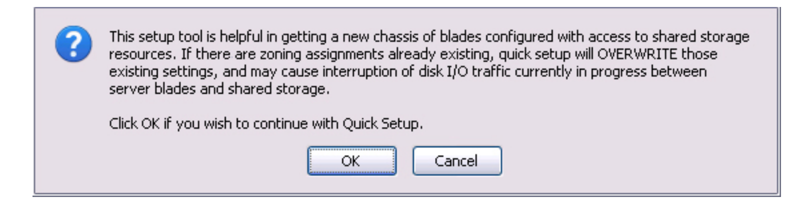
Antes de comenzar:

- Se requiere el rol Admin (a) en Oracle ILOM para modificar las propiedades de zonas SAS.
- Revise "Requisitos del hardware del chasis" en la página 250.
- Las zonas SAS deben estar activadas en Oracle ILOM antes de realizar este procedimiento de configuración rápida para la asignación de zonas. Para obtener instrucciones, consulte "Acceso y activación de Sun Blade Zone Manager " en la página 250.

1 **Para acceder a la página Sun Blade Zone Manager Settings (Configuración de Sun Blade Zone Manager) en la interfaz web, haga clic en System Management (Gestión del sistema) > SAS Zoning (Zonas SAS).**

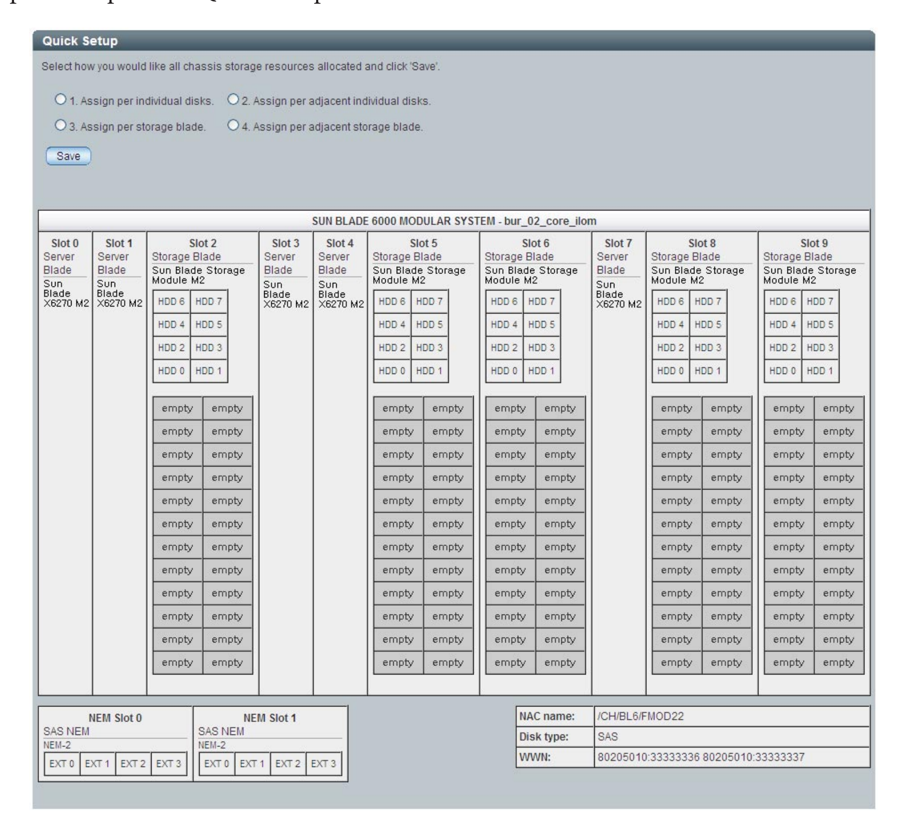
2 En la sección Sun Blade Zone Manager, haga clic en el botón Quick Setup (Configuración rápida).

A parece un mensaje de advertencia.



3 Para sobrescribir las asignaciones de zonas existentes, haga clic en OK (Aceptar).

Aparece la pantalla Quick Setup.



Nota – Las ranuras de chasis de disco duro que no tienen un disco duro actualmente instalado en el chasis se etiquetan como "empty" (vacío). Las ranuras de chasis de disco duro vacías no se incluyen en las asignaciones de almacenamiento de Quick Setup.

---

4 **Para indicar cómo desea asignar los recursos de almacenamiento de chasis, seleccione una de las opciones de Quick Setup.**

Para obtener una descripción de cada opción de Quick Setup, consulte "Whole Chassis Setup: Quick Setup (Configuración de todo el chasis: Configuración rápida)" en la página 240.

Después de elegir una opción de configuración rápida, Sun Blade Zone Manager muestra asignaciones de zonas codificadas con color entre los servidores blade de CPU y los dispositivos de almacenamiento (discos duros) instalados en los servidores blade de almacenamiento. Aunque Sun Blade Zone Manager muestre las conexiones SAS externas NEM0 y NEM1, estas conexiones no son compatibles.

Nota – Hasta que no haga clic en el botón Save (Guardar), las asignaciones de almacenamiento de chasis no se guardarán.

---

5 **Para guardar las asignaciones de almacenamiento de chasis de Quick Setup, haga clic en Save.**

6 **Para realizar una copia de seguridad de las asignaciones de grupos de almacenamiento de blade recientemente guardadas, consulte "Copia de seguridad y recuperación de asignaciones de zonas SAS-2" en la página 249.**

Más información

Información relacionada

- "Consideraciones importantes sobre las asignaciones de zonas SAS " en la página 248
- "Asignación de recursos de almacenamiento a un servidor blade único: Detailed Setup (Configuración detallada) (Web)" en la página 254
- "Asignación de recurso de almacenamiento único a varios servidores blade: Detailed Setup (Configuración detallada) (Web)" en la página 260
- "Modificación de asignaciones de grupos de blade existentes (Web)" en la página 269
- "Creación manual de asignaciones de zona SAS-2 (CLI)" en la página 264

- *Documentación del sistema modular Sun Blade 6000*

▼ Asignación de recursos de almacenamiento a un servidor blade único: Detailed Setup (Configuración detallada) (Web)

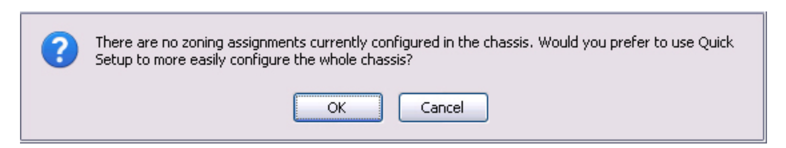
Antes de comenzar:

- Se requiere el rol Admin (a) en Oracle ILOM para modificar las propiedades de zonas SAS.
- Revise "Requisitos del hardware del chasis" en la página 250.
- Sun Blade Zone Manager debe estar activado en Oracle ILOM antes de ejecutar este procedimiento. Para obtener instrucciones, consulte "Acceso y activación de Sun Blade Zone Manager " en la página 250.

1 **En la página Sun Blade Zone Manager Settings (Configuración de Sun Blade Zone Manager), haga clic en el botón Detailed Setup (Configuración detallada).**

Aparecerá uno de los siguientes cuadros:

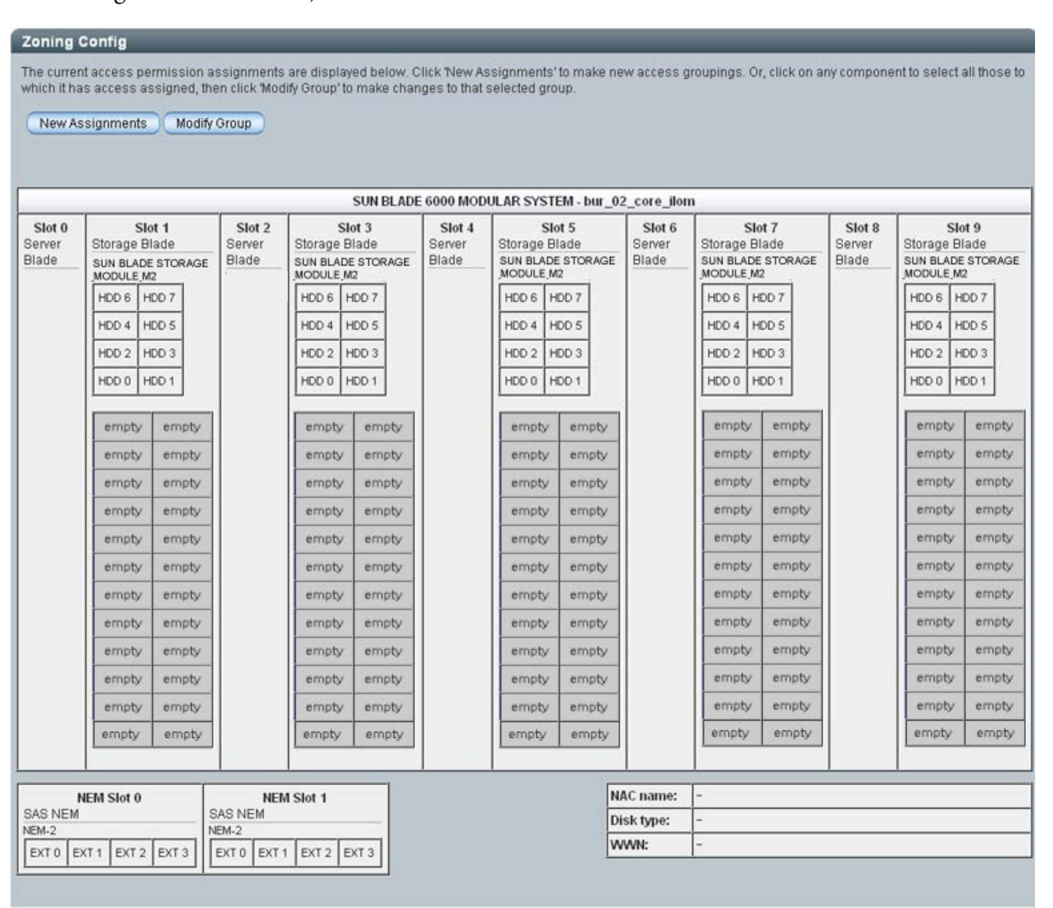
- **Aparece el diálogo Zoning Config (Configuración de zonas). Vaya al paso 3.**
- **Aparece el siguiente mensaje que indica que no existe ninguna asignación de zona. Vaya al paso 2.**



2 En el mensaje que indica que no existe ninguna asignación de zona, realice una de las siguientes acciones:

- **Si desea crear asignaciones de zonas SAS manualmente mediante la opción Detailed Setup, haga clic en Cancel (Cancelar) y vaya al paso 4.**

  Al hacer clic en Cancel, se abre la página Detailed Setup Zoning Config (Configuración de zona en configuración detallada).



- **Si desea configurar las asignaciones de zona iniciales mediante la opción Quick Setup (Configuración rápida) de Sun Blade Zone Manager, haga clic en OK (Aceptar) y vaya a** **"Asignación de almacenamiento a todo el chasis: Quick Setup (Configuración rápida) (Web)" en la página 252****.**

3 Para asignar recursos de almacenamiento a un servidor blade único, realice estos pasos en el diálogo Zoning Config:

a. Haga clic en New Assignments (Nuevas asignaciones)

Aparece el diálogo New Assignments.

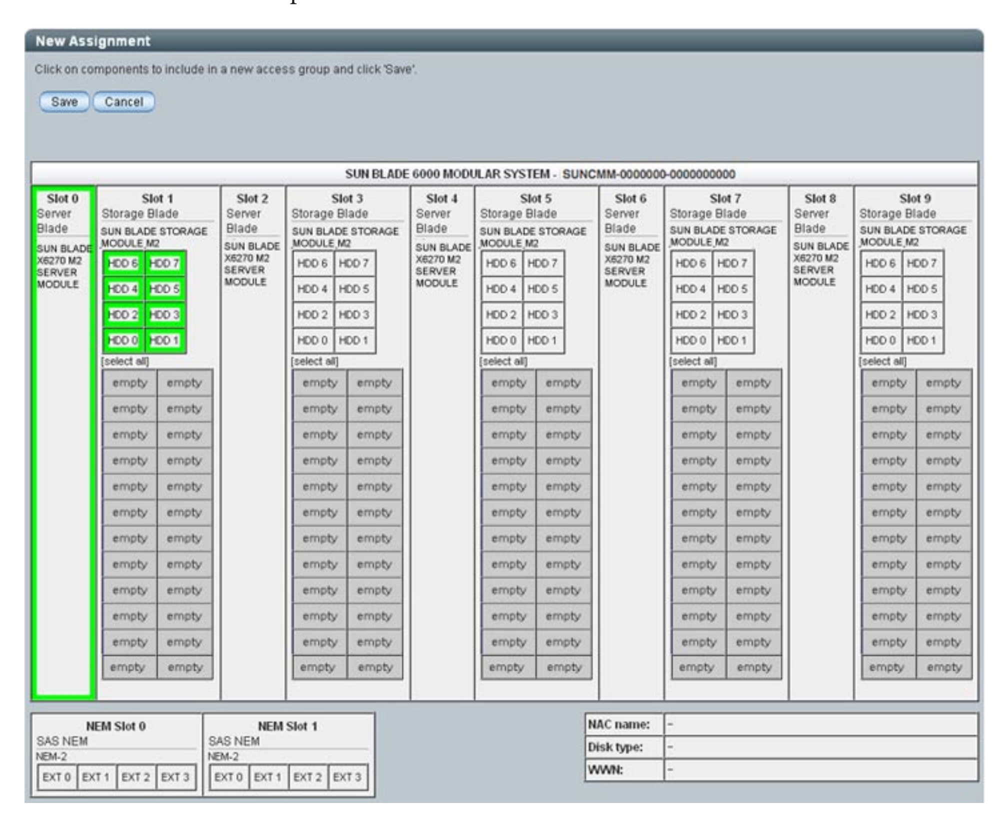
b. Haga clic en un servidor blade y luego en los recursos de almacenamiento (discos duros) que desea asignar al servidor blade seleccionado.

Nota – Todas las ranuras de chasis de disco duro que no tengan un dispositivo de almacenamiento de disco duro instalado se etiquetarán como "empty" (vacío). Las ranuras de chasis de disco duro vacías no se asignan a los servidores blade de CPU.

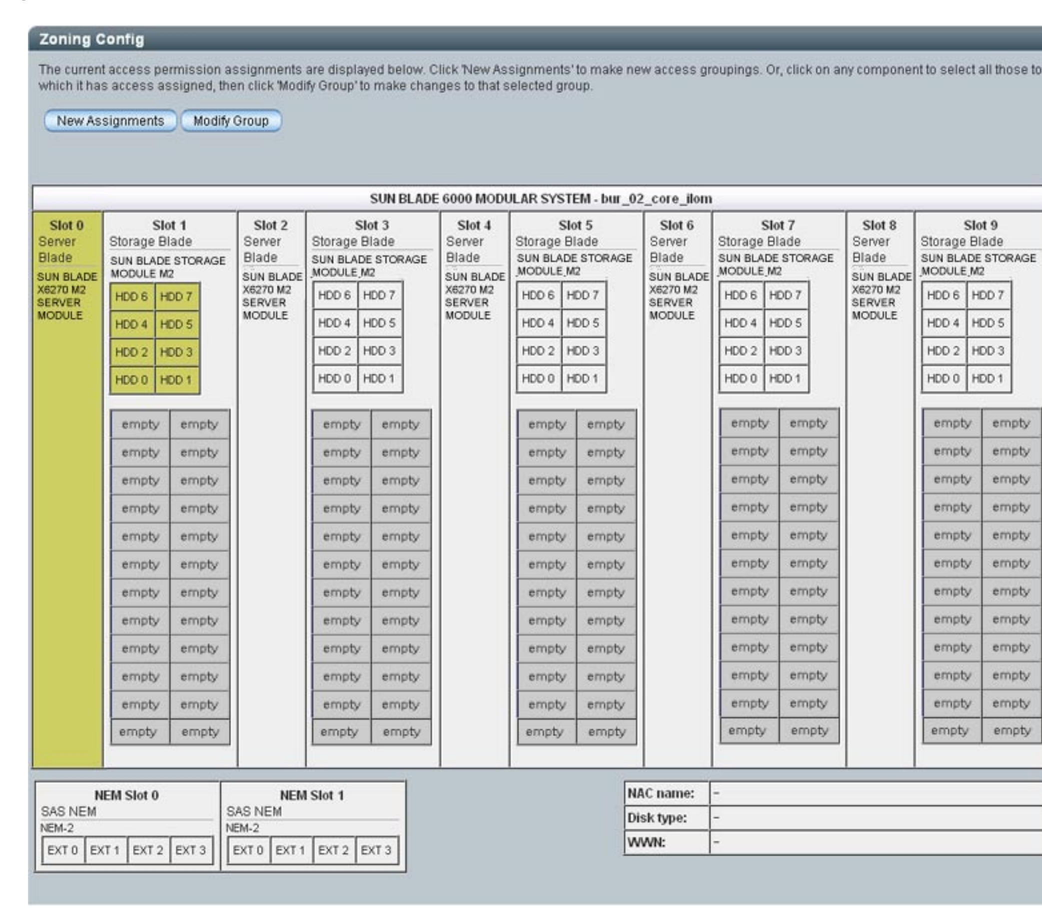


Precaución – De manera alternativa, puede asignar recursos de almacenamiento a varios servidores blade; sin embargo, los servidores deben estar activados para múltiples rutas. Para obtener más instrucciones, consulte "Asignación de recurso de almacenamiento único a varios servidores blade: Detailed Setup (Configuración detallada) (Web)" en la página 260.

Aunque Sun Blade Zone Manager muestre las conexiones SAS externas NEM0 y NEM1, estas conexiones no son compatibles.



c. **Para guardar la asignación de grupos de almacenamiento de blade recientemente creada, haga clic en Save.**



4 **Para realizar una copia de seguridad de las asignaciones de grupos de almacenamiento de blade recientemente guardadas, consulte** **"Copia de seguridad y recuperación de asignaciones de zonas SAS-2" en la página 249****.**

Más información

Información relacionada

- "Modificación de asignaciones de grupos de blade existentes (Web)" en la página 269
- "Consideraciones importantes sobre las asignaciones de zonas SAS " en la página 248
- "Asignación de recurso de almacenamiento único a varios servidores blade: Detailed Setup (Configuración detallada) (Web)" en la página 260
- *Documentación del sistema modular Sun Blade 6000*

▼ Asignación de recurso de almacenamiento único a varios servidores blade: Detailed Setup (Configuración detallada) (Web)

Antes de empezar



Precaución – Consulte la documentación del servidor Sun Blade para determinar si el módulo de servidor Sun Blade está activado para compartir recursos de almacenamiento con otro módulo de servidor Sun Blade.

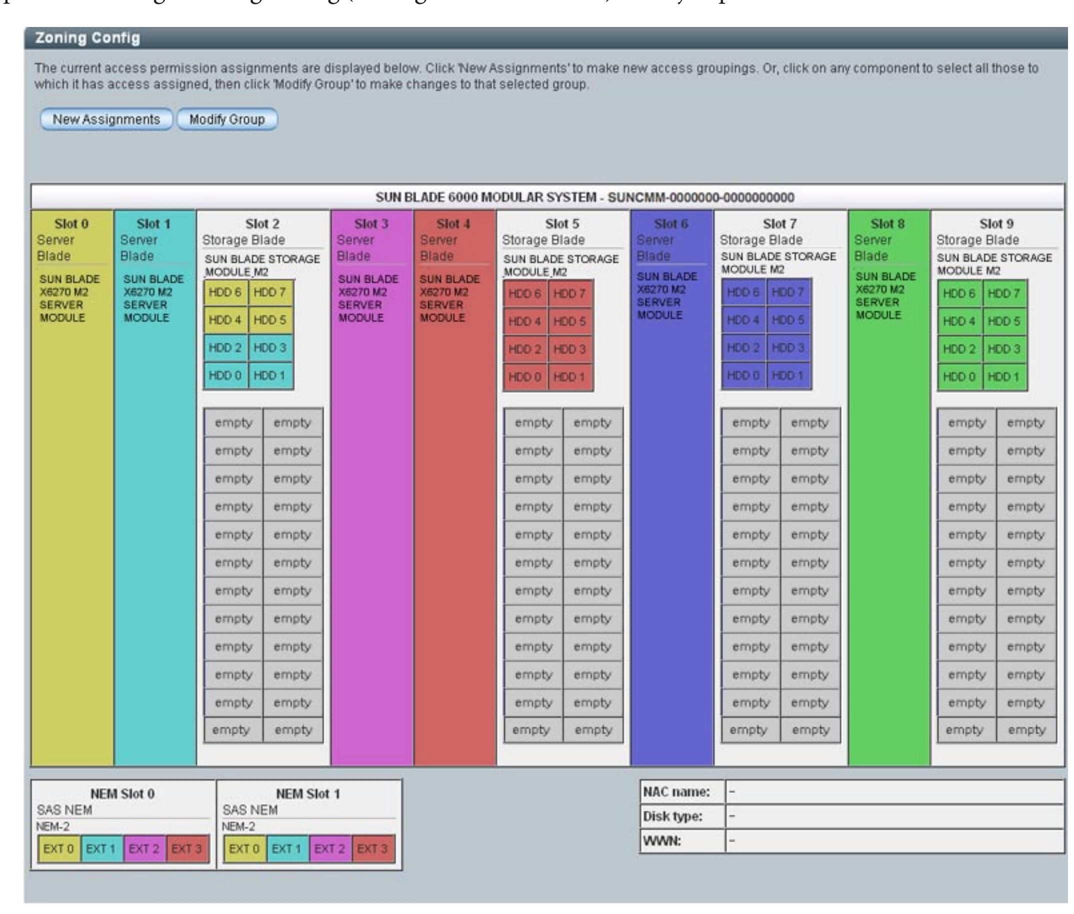


Precaución – La opción para compartir un recurso de almacenamiento único sólo se utiliza con una solución de agrupación en clústeres compatible con Oracle. Para obtener más información sobre las soluciones de agrupación en clústeres, consulte la *Guía de administración de módulos de almacenamiento Sun Blade*.

- Se requiere el rol Admin (a) en Oracle ILOM para modificar las propiedades de zonas SAS.
- Revise "Requisitos del hardware del chasis" en la página 250.
- Sun Blade Zone Manager debe estar activado en Oracle ILOM antes de ejecutar este procedimiento. Para obtener instrucciones, consulte "Acceso y activación de Sun Blade Zone Manager " en la página 250.

1 **En la página Sun Blade Zone Manager Settings (Configuración de Sun Blade Zone Manager), haga clic en el botón Detailed Setup (Configuración detallada).**

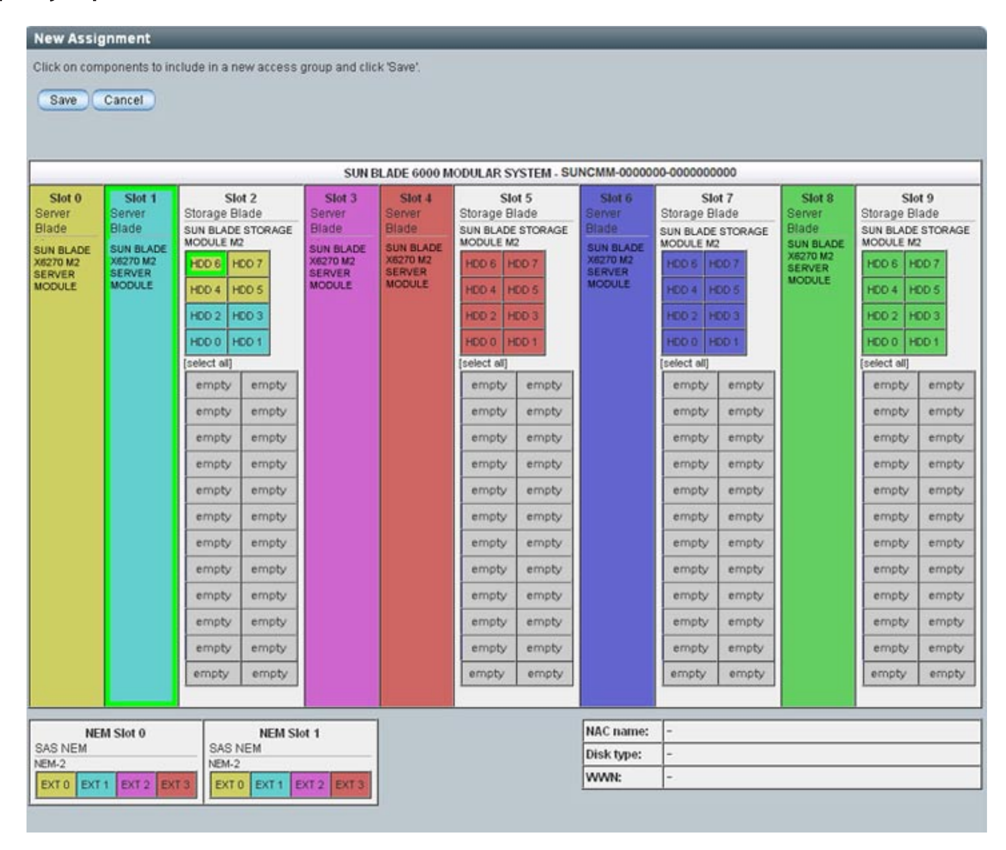
Aparece el diálogo Zoning Config (Configuración de zonas). Por ejemplo:



2 **Para asignar un recurso de almacenamiento único a varios servidores blade, realice los siguientes pasos:**

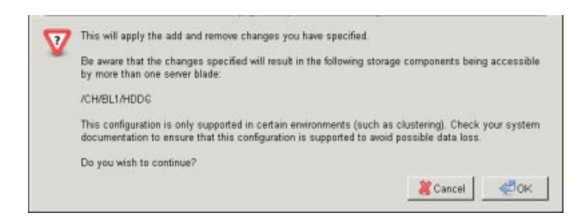
a. **Haga clic en New Assignments (Nuevas asignaciones)**

b. **Para compartir un recurso de blade de almacenamiento único (por ejemplo, HEDA en la ranura 2) actualmente asignado a un servidor blade único (por ejemplo, en la ranura 0) con otro servidor blade (por ejemplo, en la ranura 1), haga clic en el destino de servidor blade adicional (por ejemplo, en la ranura 1) y luego haga clic en el recurso de blade de almacenamiento (por ejemplo, HEDA en la ranura 2) que desea compartir con este destino (por ejemplo, en la ranura 1).**



c. **Para guardar la modificación en la asignación al grupo de almacenamiento de blade, haga clic en Save (Guardar).**

Aparece el siguiente mensaje.

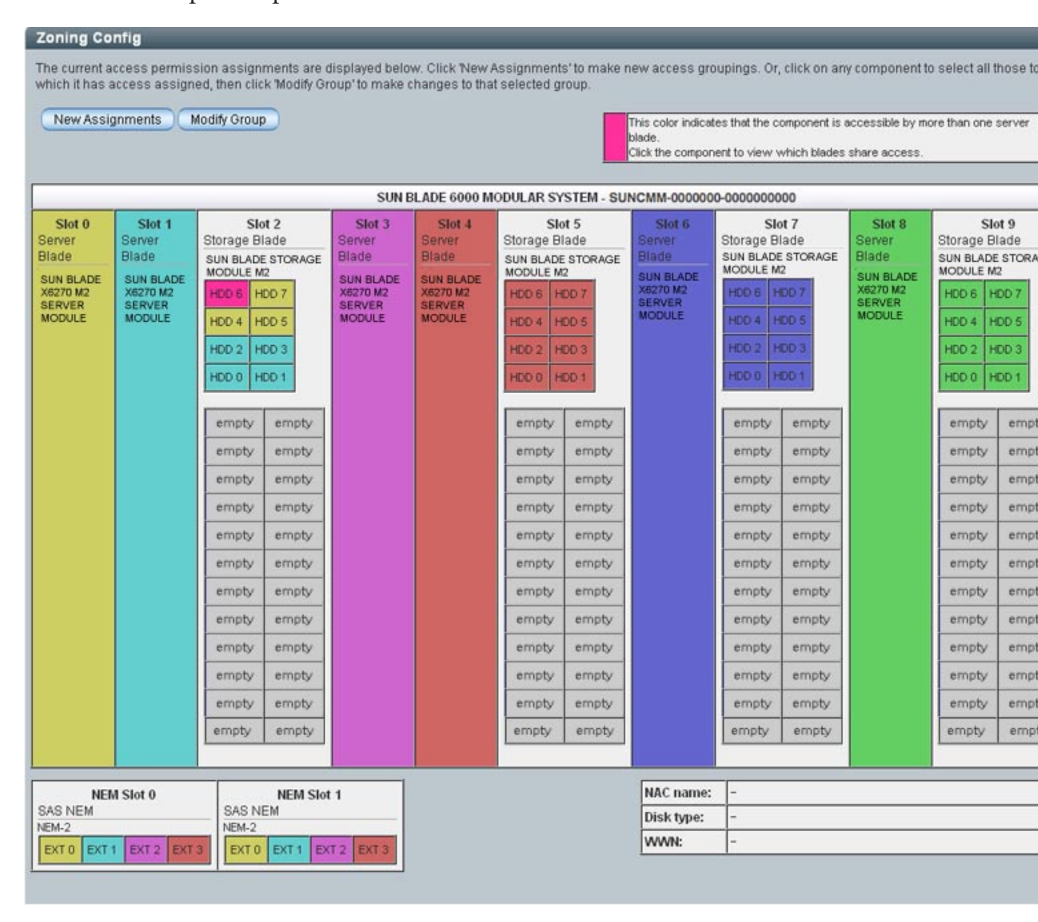


d. **Para continuar guardando la asignación de grupos de almacenamiento de blade, haga clic en OK (Aceptar)**

Sun Blade Zone Manager resalta los recursos de almacenamiento compartidos en rosa.

Ejemplo:

El recurso de almacenamiento HEDA en la ranura 2 está resaltado en rosa para indicar que este recurso es compartido por más de un servidor blade de CPU.



3 **Para realizar una copia de seguridad de los grupos de almacenamiento de blade recientemente asignados, consulte “Copia de seguridad y recuperación de asignaciones de zonas SAS-2” en la página 249.**

Más información Información relacionada

- “Consideraciones importantes sobre las asignaciones de zonas SAS ” en la página 248
- “Gestión de asignaciones de recursos de almacenamiento SAS-2 existentes” en la página 266
- *Documentación del sistema modular Sun Blade 6000*

Creación manual de asignaciones de zona SAS-2 (CLI)

Antes de empezar

- Asegúrese de que su configuración de chasis cumpla con los requisitos estipulados en “Requisitos del hardware del chasis” en la página 250.
- Se requieren privilegios del rol Admin (a) para crear manualmente asignaciones de zonas SAS en Oracle ILOM.
- Sun Blade Zone Manager debe estar activado en Oracle ILOM.

1. **Acceda a Sun Blade Zone Manager desde la CLI.**

   Para obtener instrucciones, consulte “Acceso y activación de Sun Blade Zone Manager ” en la página 250.

2. **Utilice uno de los siguientes métodos para asignar un recurso de almacenamiento a un servidor blade de CPU:**

   - **Método 1**: Para asignar un disco de almacenamiento a un servidor blade de CPU, utilice los siguientes comandos:

     -> **Cd /STORAGE/sas_zoning/BL***n*

     -> **set add_storage_access=***path_to_storage_disk*

     Donde BL*n* es el número de ranura del chasis para el servidor blade de CPU y *path_to_storage_disk* es la ruta al disco de blade de almacenamiento que desea asignar al servidor blade de CPU.

     Por ejemplo, para asignar el disco duro en la ubicación de ranura de blade de almacenamiento 0 al servidor blade de CPU en la ubicación de ranura de chasis 1, debería escribir:

     -> **set add_storage_access=/CH/BL1/HDD0**.

   - **Método 2**: Para asignar el servidor blade de CPU a un recurso de almacenamiento, escriba:

     -> **Cd /STORAGE/sas_zoning/BL***n***/HDD***n*

     -> **set add_host_access=***path_to_blade_server*

     Donde BL*n* es la ubicación de ranura de chasis para el servidor blade de CPU, HDD*n* es la ubicación de ranura de blade de almacenamiento para el disco duro y *path_to_blade_server* es el destino de servidor blade de CPU a donde desea asignar el disco de almacenamiento.

Por ejemplo, si desea asignar un disco duro dentro de un servidor blade de almacenamiento a un servidor blade de CPU en el chasis, debería escribir:

-> **Cd /STORAGE/sas_zoning/BL1/HDD0**

-> **set add_host_access=/CH/BL0**

Los siguientes ejemplos muestran cómo utilizar estos comandos para configurar asignaciones de zonas entre dispositivos de almacenamiento en un blade de almacenamiento en la ranura 1 y en un blade de servidor en la ranura 0.

- **Método 1**: ejemplos de comandos para asignar recursos de almacenamiento a un servidor blade de CPU.

Ejemplos de sintaxis de comandos de la CLI	Instrucciones
-> **cd /STORAGE/sas_zoning/BL0**	a. Utilice este primer ejemplo de sintaxis de comandos para acceder al servidor blade de CPU que se asignará a un recurso de almacenamiento.
-> **set add_storage_access=/CH/BL1/HDD0**	b. Utilice el segundo ejemplo de sintaxis de comandos para asignar el módulo de almacenamiento (HDD0) en el servidor blade de almacenamiento (BL1) al servidor blade de CPU del host (BL0) en la ranura de chasis 0.
-> **set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1**	c. De manera opcional, puede utilizar la tercera sintaxis de comandos para asignar varios dispositivos en una única línea de comandos. Asegúrese de especificar la ruta completa al recurso de almacenamiento y separar cada recurso con una coma (sin espacio).
-> **show** /STORAGE/sas_zoning/BL0 Destinos: 0 (/CH/BL1/HDD0) 1 (/CH/BL1/HDD1)	d. Utilice el comando show para confirmar que las asignaciones de almacenamiento se guardan en el servidor blade de CPU (/CH/BL1/HD0 y CH/BL1/HDD1).

- **Método 2**: ejemplos de comandos para asignar una blade de servidor de CPU (BL0) a un recurso de blade de almacenamiento (BL1/HDD0):

Ejemplos de sintaxis de comandos de la CLI	Instrucciones
`-> cd /STORAGE/sas_zoning/BL1/HDD0`	a. Utilice el primer ejemplo de sintaxis de comandos para acceder al recurso de almacenamiento (HDD0) instalado en el servidor blade de almacenamiento (BL1/HDD0).
`-> set add_host_access=/CH/BL0`	b. Utilice el segundo ejemplo de sintaxis de comandos para asignar el recurso de almacenamiento (HDD0) al servidor blade de CPU del host (BL0).

`-> show`
`/STORAGE/sas_zoning/BL1/HDD0`
`Destinos:`
`0 (/CH/BL0)`
	c. Utilice el comando `show` para confirmar que las asignaciones de almacenamiento se guardan en el servidor blade de CPU correcto (/CH/BL0).

3 Realice una copia de seguridad del grupo de almacenamiento de servidor recientemente guardado.

Más información

Información relacionada

- "Copia de seguridad y recuperación de asignaciones de zonas SAS-2" en la página 249
- "Creación manual de asignaciones de zona SAS-2 (CLI)" en la página 264
- *Documentación del sistema modular Sun Blade 6000*

Gestión de asignaciones de recursos de almacenamiento SAS-2 existentes

Sun Blade Zone Manager en Oracle ILOM permite gestionar las asignaciones existentes a los recursos de almacenamiento de chasis en las siguientes formas:

- "Visualización de asignaciones de almacenamiento de servidor blade de CPU existentes (Web)" en la página 266
- "Modificación de asignaciones de grupos de blade existentes (Web)" en la página 269
- "Visualización y modificación de asignaciones de almacenamiento existentes (CLI)" en la página 273

▼ Visualización de asignaciones de almacenamiento de servidor blade de CPU existentes (Web)

Antes de empezar

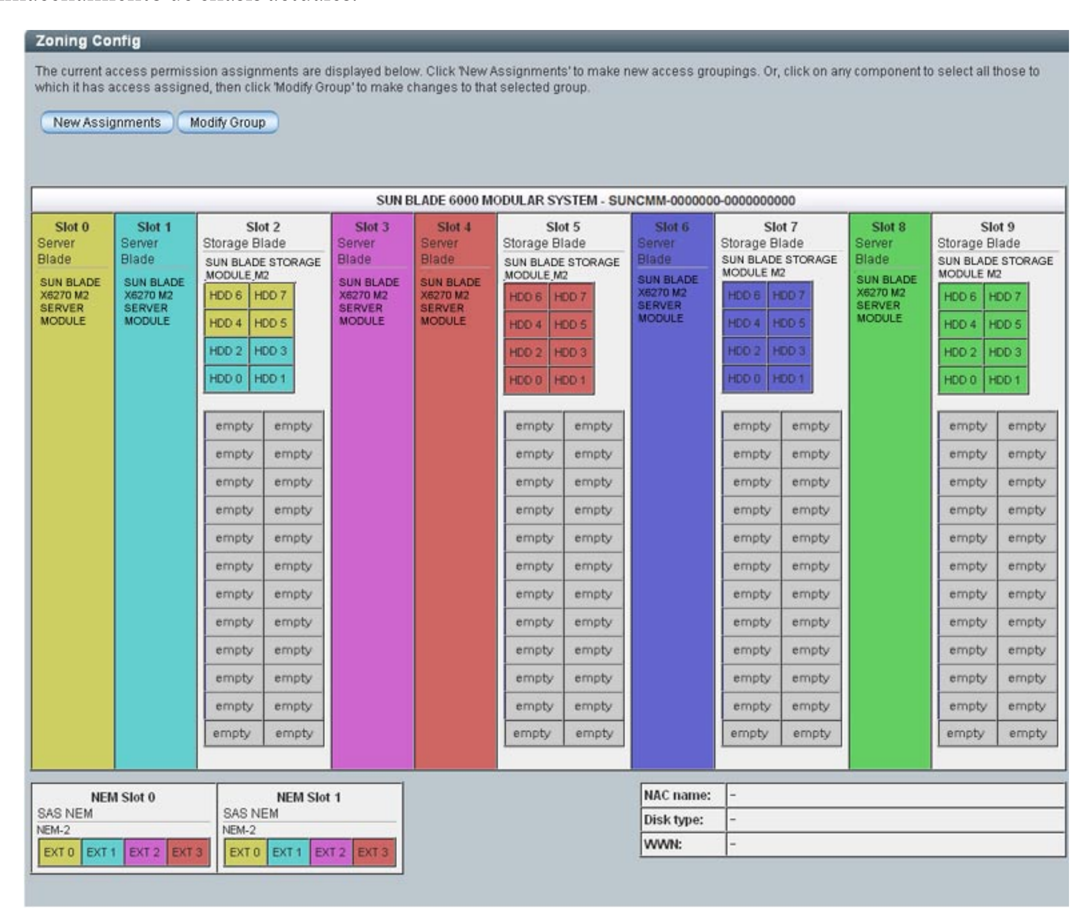
- Se requieren privilegios del rol Admin (a) para ver asignaciones de Sun Blade Zone Manager en Oracle ILOM.

- Sun Blade Zone Manager debe estar activado en Oracle ILOM.

1 **Acceda a Sun Blade Zone Manager y haga clic en Detailed Setup (Configuración detallada).**

Para obtener instrucciones para acceder a Sun Blade Zone Manager, consulte "Acceso y activación de Sun Blade Zone Manager " en la página 250.

Aparece el diálogo Zoning Config (Configuración de zona) que muestra las asignaciones de almacenamiento de chasis actuales.



2 **Para ver todas las asignaciones de recursos para un servidor blade de CPU seleccionado, realice estos pasos:**

a. **Seleccione una ranura de servidor blade de CPU.**

Para este ejemplo, se ha seleccionado la ranura 0.

b. Desplácese hacia abajo hasta la tabla Current Assignments (Asignaciones actuales)

Todos los recursos de almacenamiento actualmente asignados al servidor blade de CPU seleccionado se muestran en la tabla Current Assignments.

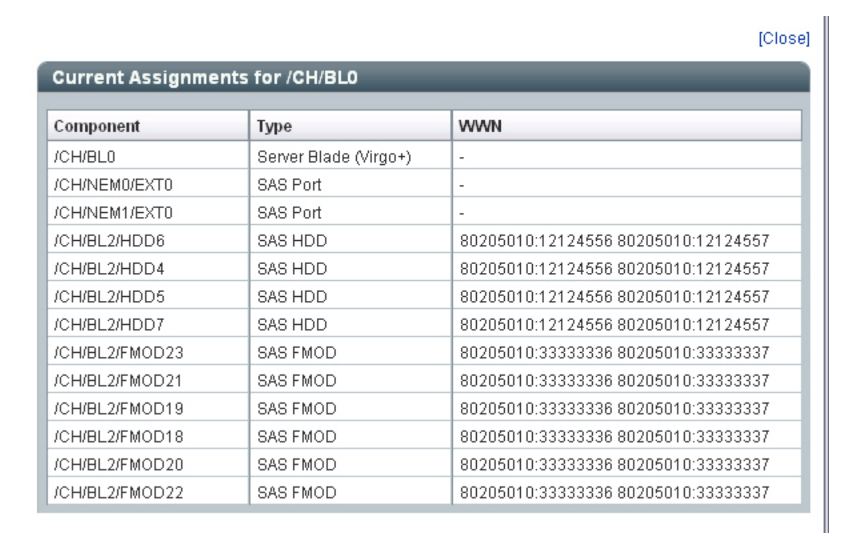
Current Assignments for /CH/BL0

Detach Table

Component	Type	WWN
/CH/BL0	Server Blade (Virgo+)	-
/CH/NEM0/EXT0	SAS Port	-
/CH/NEM1/EXT0	SAS Port	-
/CH/BL2/HDD6	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD4	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD5	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD7	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/FMOD23	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD21	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD19	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD18	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD20	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD22	SAS FMOD	80205010:33333336 80205010:33333337

3 **Para ver, al mismo tiempo, la tabla Current Assignments para el servidor blade de CPU seleccionado y las asignaciones de recursos para otros servidores blade de CPU de chasis, haga clic en Detach Table (Desvincular tabla).**

Aparece la tabla Current Assignments desvinculada en un cuadro de diálogo separado.



[Close]

Current Assignments for /CH/BL0

Component	Type	WWN
/CH/BL0	Server Blade (Virgo+)	-
/CH/NEM0/EXT0	SAS Port	-
/CH/NEM1/EXT0	SAS Port	-
/CH/BL2/HDD6	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD4	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD5	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD7	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/FMOD23	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD21	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD19	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD18	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD20	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD22	SAS FMOD	80205010:33333336 80205010:33333337

Más información

Información relacionada

- “Modificación de asignaciones de grupos de blade existentes (Web)” en la página 269
- “Consideraciones importantes sobre las asignaciones de zonas SAS ” en la página 248
- “Creación manual de asignaciones de zona SAS-2 (CLI)” en la página 264

- *Documentación del sistema modular Sun Blade 6000*

▼ Modificación de asignaciones de grupos de blade existentes (Web)

Antes de empezar

Antes de empezar

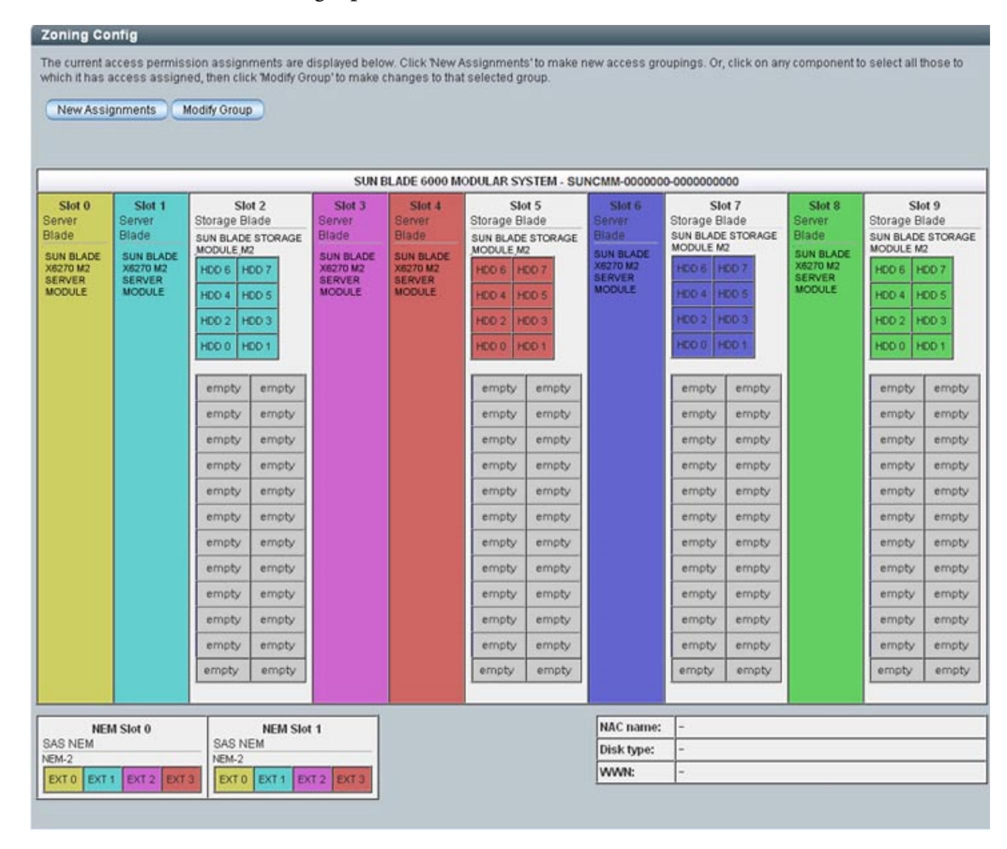
- Asegúrese de que su configuración de hardware del chasis cumpla con los requisitos descritos en "Requisitos del hardware del chasis" en la página 250.
- Se requieren privilegios del rol Admin (a) en Oracle ILOM para modificar cualquiera de las propiedades de Sun Blade Zone Manager.
- Sun Blade Zone Manager debe estar activado en Oracle ILOM.

1 **Para acceder a Sun Blade Zone Manager, haga clic en System Management (Gestión del sistema) > SAS Zoning (Zonas SAS).**

Aparece la página SAS Zoning.

2 En la sección Sun Blade Zone Manager, haga clic en Detailed Setup (Configuración detallada).

Aparece el diálogo Zoning Config (Configuración de zona) que muestra las asignaciones de almacenamiento existentes en grupos codificados con color.

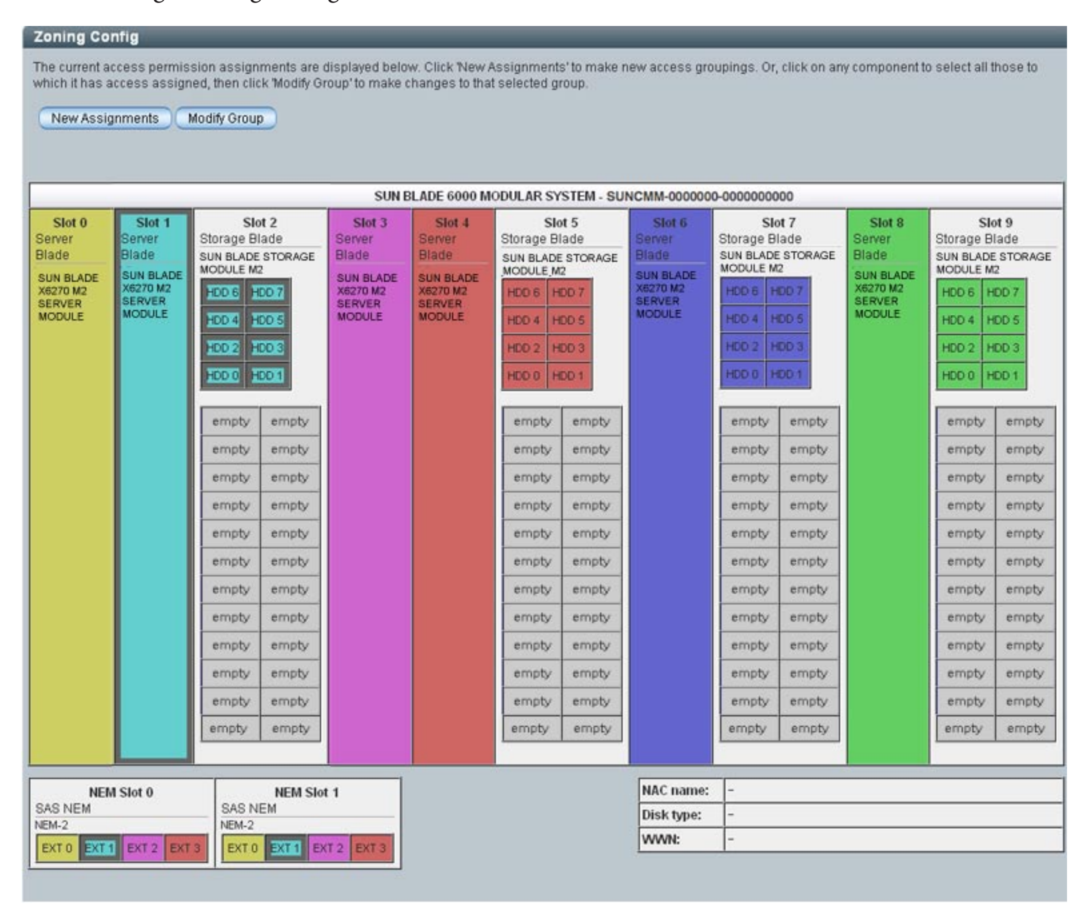


Nota – Las ranuras de HDD que no tengan un dispositivo de almacenamiento instalado se etiquetarán como "empty" (vacío). Las ranuras de disco duro vacías no se asignan a los servidores blade de CPU.

---

3 Para modificar las asignaciones de almacenamiento para un grupo de almacenamiento de blade, seleccione un blade que forme parte del grupo.

Sun Blade Zone Manager resalta el almacenamiento asignado al grupo de almacenamiento de blade en el diálogo Zoning Config.



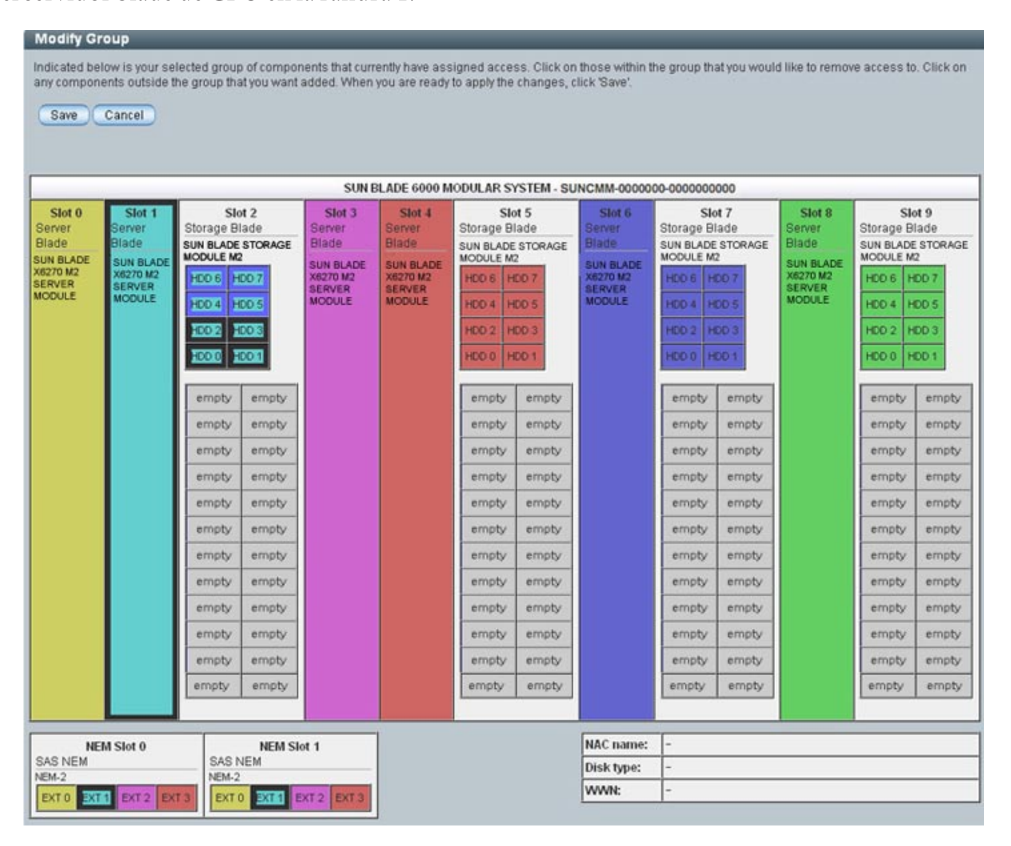
4 Para modificar los recursos de almacenamiento asignados a un grupo de almacenamiento de blade seleccionado, haga clic en Modify Group (Modificar grupo).

Sun Blade Zone Manager resalta el grupo de almacenamiento de blade seleccionado (que incluye los recursos de almacenamiento actualmente asignados al servidor blade de CPU).

5 Realice una o varias de las siguientes modificaciones de almacenamiento al grupo seleccionado:

- **Para eliminar los recursos de almacenamiento asignados a un grupo de almacenamiento de blade seleccionado, haga clic en los recursos que desea eliminar.**

  Ejemplo: La siguiente ilustración muestra HDD 4-7 como recursos seleccionados a eliminar del servidor blade de CPU en la ranura 1.



- **Para asignar recursos de almacenamiento adicionales a un grupo de almacenamiento de blade, haga clic en cualquier recurso de almacenamiento fuera del grupo codificado con color que desea agregar.**

6 Para aplicar las modificaciones realizadas al grupo de almacenamiento de blade seleccionado, haga clic en Save (Guardar).

7 Realice una copia de seguridad de las asignaciones de recursos modificadas y guardadas recientemente.

Más información

Información relacionada

- “Consideraciones importantes sobre las asignaciones de zonas SAS ” en la página 248
- “Copia de seguridad y recuperación de asignaciones de zonas SAS-2” en la página 249
- “Visualización y modificación de asignaciones de almacenamiento existentes (CLI)” en la página 273
- *Documentación del sistema modular Sun Blade 6000*

▼ Visualización y modificación de asignaciones de almacenamiento existentes (CLI)

Antes de empezar

Antes de empezar

- Asegúrese de que su configuración de hardware de chasis cumpla con los requisitos estipulados en “Requisitos del hardware del chasis” en la página 250.
- Se requieren privilegios del rol Admin (a) en Oracle ILOM para ver y modificar las propiedades de Sun Blade Zone Manager.
- Sun Blade Zone Manager debe estar activado en Oracle ILOM.

1 Acceda a Sun Blade Zone Manager desde la CLI.

Consulte “Acceso y activación de Sun Blade Zone Manager ” en la página 250.

2 Para ver los recursos de almacenamiento asignados a un servidor blade de CPU, realice una de las siguientes acciones:

- **Para ver las asignaciones de almacenamiento de un servidor blade de CPU, utilice el comando `show` seguido del destino `/STORAGE/sas_zoning/BL`*n*. Por ejemplo:**

  ```
  -> show /STORAGE/sas_zoning/BL0

     Targets:
        0     (/CH/BL2/HDD0)
        1     (/CH/BL2/HDD1)
  ```

  En este ejemplo, HDD0 y HDD1, que actualmente están instalados en el servidor blade de almacenamiento en la ranura de chasis 2, se asignan al servidor blade de CPU en la ranura de chasis 0.

- **Para ver el lugar en el que está asignado un recurso de blade de almacenamiento, utilice el comando `show` seguido del destino `/STORAGE/BL`*n*`/HDD`*n*. Por ejemplo:**

  ```
  -> show /STORAGE/BL2/HDD0

     Targets:
        0     (/CH/BL0)

  -> show /STORAGE/BL2/HDD1
  ```

```
Targets:
   0     (/CH/BL0)
```

En este ejemplo, los recursos HDD0 y HDD1, que están instalados en el servidor blade de almacenamiento en la ranura de chasis 2, se asignan al servidor blade de CPU en la ranura de chasis 0.

3 **Para modificar las asignaciones de almacenamiento, realice uno de los siguientes métodos:**

Método 1: adición o anulación de la asignación de recursos de almacenamiento por servidor blade de CPU.

- Para asignar un recurso de almacenamiento a un servidor blade de CPU, escriba:

  -> **cd /STORAGE/sas_zoning/BL***n* -> **set add_storage_access=***path_to_storage_device*

  Donde BL*n* es la ubicación de la ranura de chasis de servidor blade de CPU y *path_to_storage_device* es la ruta al recurso de blade de almacenamiento.

- Para anular la asignación de un recurso de almacenamiento de un servidor blade de CPU, escriba:

  -> **cd /STORAGE/sas_zoning/BL***n* -> **set remove_storage_access=***path_to_storage_device*

  Donde BL*n* es la ubicación de la ranura de chasis de servidor blade de CPU y *path_to_storage_device* es la ruta al recurso de servidor blade de almacenamiento. Por ejemplo, `/CH/BL1/HDD0`.

Método 2: adición o anulación de la asignación de acceso de servidor blade al dispositivo de almacenamiento.

- Para asignar un servidor blade de CPU a un recurso de almacenamiento, escriba:

  -> **cd /STORAGE/sas_zoning/BL***n***/HDD***n*

  -> **set add_host_access=***path_to_blade_server*

- Para anular la asignación del acceso de un servidor blade de host a un dispositivo de almacenamiento, escriba:

  -> **cd /STORAGE/sas_zoning/BL***n***/HDD***n*

  -> **set remove_host_access=***path_to_blade_server*

Donde BL*n* es la ubicación de la ranura de chasis de servidor blade de almacenamiento, HDD*n* es la ubicación de la ranura de recursos de almacenamiento y *path_to_blade_server* es la ubicación de la ranura de chasis para el servidor blade de CPU al que desea asignar el recurso del que desea anular su asignación. Por ejemplo, `/CH/BL0`.

Nota – También puede agregar o anular la asignación de varios dispositivos de almacenamiento en una sola línea de comandos. Para ello, especifique la ruta completa al recurso y separe cada recurso con una coma (sin espacio). Por ejemplo: `->` **`set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1`**

4 **Realice una copia de seguridad de la asignación del grupo de almacenamiento de blade.**

Más información

Información relacionada

- "Consideraciones importantes sobre las asignaciones de zonas SAS " en la página 248
- "Copia de seguridad y recuperación de asignaciones de zonas SAS-2" en la página 249
- "Creación manual de asignaciones de zona SAS-2 (CLI)" en la página 264

- *Documentación del sistema modular Sun Blade 6000*

Restablecimiento de asignaciones de Sun Blade Zone Manager a los valores predeterminados de fábrica

Para borrar todas las asignaciones de almacenamiento de chasis guardadas de Sun Blade Zone Manager e iniciar Sun Blade Zone Manager desde los valores predeterminados de fábrica, realice uno de los siguientes procedimientos.

- "Restablecimiento de las asignaciones de zona a los valores predeterminados de fábrica (Web) " en la página 275
- "Restablecimiento de las asignaciones de zona a los valores predeterminados de fábrica (CLI) " en la página 276

▼ Restablecimiento de las asignaciones de zona a los valores predeterminados de fábrica (Web)

Antes de empezar

Antes de empezar

- Se requieren privilegios del rol Admin (a) en Oracle ILOM para modificar las propiedades de Sun Blade Zone Manager.



Precaución – Utilice este procedimiento sólo si desea borrar todas las asignaciones de zonas SAS actualmente guardadas en Oracle ILOM.

1 **Para acceder a la página de Sun Blade Zone Manager en la interfaz web del CMM, haga clic en System Management (Gestión del sistema) > SAS Zoning (Zonas SAS).**

Si el estado de Sun Blade Manager está activado, aparece el botón Reset All (Restablecer todo) en la sección Zoning Reset (Restablecimiento de zona) de la página de Sun Blade Zone Manager.

2 Para borrar todas las asignaciones de recursos guardadas y restablecer Sun Blade Zone Manager a los valores predeterminados de fábrica, haga clic en Reset All.

Restablecimiento de las asignaciones de zona a los valores predeterminados de fábrica (CLI)

Antes de empezar

Antes de empezar

- Se requieren privilegios del rol Admin (a) en Oracle ILOM para modificar las propiedades de Sun Blade Zone Manager.



Precaución – Utilice este procedimiento sólo si desea borrar todas las asignaciones de zonas SAS actualmente guardadas en Oracle ILOM.

1 Navegue hasta `/STORAGE/sas_zoning` en la CLI del CMM mediante el siguiente comando:

```
-> cd /STORAGE/sas_zoning
```

2 Para borrar todas las asignaciones de recursos guardadas y restablecer Sun Blade Zone Manager a los valores predeterminados de fábrica, escriba:

```
-> set reset_access_action=true
```

Si Zone Manager está desactivado, obtendrá la siguiente advertencia:

```
set: The CMM is not the SAS Zone Manager (El CMM no es el Zone Manager de SAS)
```

Si recibe este mensaje, habilite Zone Manager y vuelva a ejecutar el comando restablecer. Para más información, consulte "Acceso y activación de Sun Blade Zone Manager " en la página 250.

Restablecimiento de la contraseña de zona al valor predeterminado de fábrica para gestión en banda de terceros

Si está gestionando asignaciones de almacenamiento para dispositivos de almacenamiento en el nivel de chasis mediante una aplicación de gestión de zonas en banda de terceros y necesita restablecer la contraseña de gestión de zonas al valor predeterminado de fábrica, realice uno de los siguientes procedimientos.

- "Restablecimiento de la contraseña de zonas (Web)" en la página 276
- "Restablecimiento de la contraseña de zonas (CLI)" en la página 277

Restablecimiento de la contraseña de zonas (Web)

Antes de empezar

Antes de empezar

- Se requieren privilegios del rol Admin (a) en Oracle ILOM para modificar las propiedades de Sun Blade Zone Manager.



Precaución – Utilice este procedimiento sólo si no utiliza Oracle ILOM Zone Manager y utiliza una aplicación de gestión en banda de terceros para gestionar las asignaciones de almacenamiento de chasis.

1. **Para verificar que el estado de Sun Blade Zone Manager esté desactivado en la interfaz web del CMM, haga clic en System Management (Gestión del sistema) > SAS Zoning (Zonas SAS).**

   Aparecerá la página de Sun Blade Zone Manager.

   Si Sun Blade Zone Manager está desactivado, aparece una opción para restablecer la contraseña en la sección In-band Zoning Manager (Gestor de zonas en banda).

2. **Para restablecer la contraseña de zonas al valor predeterminado (todos ceros), haga clic en Reset (Restablecer).**

▼ Restablecimiento de la contraseña de zonas (CLI)

Antes de empezar

Antes de empezar

- Se requieren privilegios del rol Admin (a) en Oracle ILOM para modificar las propiedades de Sun Blade Zone Manager.



Precaución – Utilice este procedimiento sólo si no utiliza Oracle ILOM Zone Manager y utiliza una aplicación de gestión en banda de terceros para gestionar las asignaciones de almacenamiento de chasis.

1. **Navegue hasta `/STORAGE/sas_zoning` mediante el siguiente comando:**

```
-> cd /STORAGE/sas_zoning
```

2. **Para restablecer la contraseña de zonas actual, escriba:**

```
-> set reset_password_action=true
```

   La contraseña se establece en el valor predeterminado (todo ceros).

Índice

T